

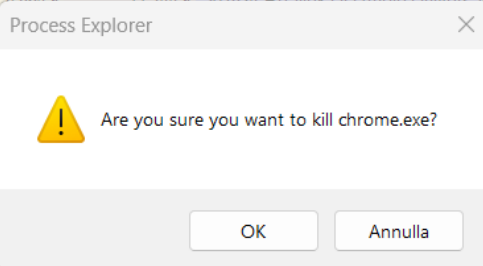
## Esplorazione di Processi, Thread, Handle e Registro di Windows

In questo laboratorio, esploreremo i processi, i thread e gli handle utilizzando Process Explorer nella suite SysInternals. Utilizzeremo anche il Registro di Windows per modificare un'impostazione.

È possibile terminare il processo, in questo caso di Google Chrome, direttamente in Process Explorer. Per farlo, fare clic con il pulsante destro del mouse sul processo identificato e selezionare l'opzione "Kill Process". Confermare l'operazione cliccando su "OK" nella finestra di dialogo che

ProtonDrive.exe	< 0.01	141.544 K	29.804 K	306224	Proton Drive	Proton AG
chrome.exe	< 0.01	126.320 K	227.432 K	321588	Google Chrome	Google LLC
chrome.exe		2.276 K	2.440 K	300848	Google Chrome	Google LLC
chrome.exe	0.12	226.200 K	126.564 K	312952	Google Chrome	Google LLC
chrome.exe		25.228 K	40.424 K	267724	Google Chrome	Google LLC
chrome.exe		10.796 K	9.528 K	313696	Google Chrome	Google LLC
chrome.exe		33.896 K	34.784 K	325092	Google Chrome	Google LLC
chrome.exe	0.12	162.980 K	167.836 K	318104	Google Chrome	Google LLC
chrome.exe		9.032 K	11.652 K	310240	Google Chrome	Google LLC
chrome.exe		11.216 K	32.544 K	261812	Google Chrome	Google LLC
chrome.exe	0.98	216.364 K	224.020 K	315076	Google Chrome	Google LLC
chrome.exe		45.640 K	103.596 K	329148	Google Chrome	Google LLC
chrome.exe		13.948 K	30.808 K	328544	Google Chrome	Google LLC
VirtualBox.exe	< 0.01	91.296 K	123.124 K	325144	VirtualBox Manager	Oracle and/or its affiliates
procexp.exe		5.928 K	15.092 K	306552	Sysinternals Process Explorer	Sysinternals - www.sysinter...
procexp64.exe	0.25	292.428 K	326.744 K	325044	Sysinternals Process Explorer	Sysinternals - www.sysinter...

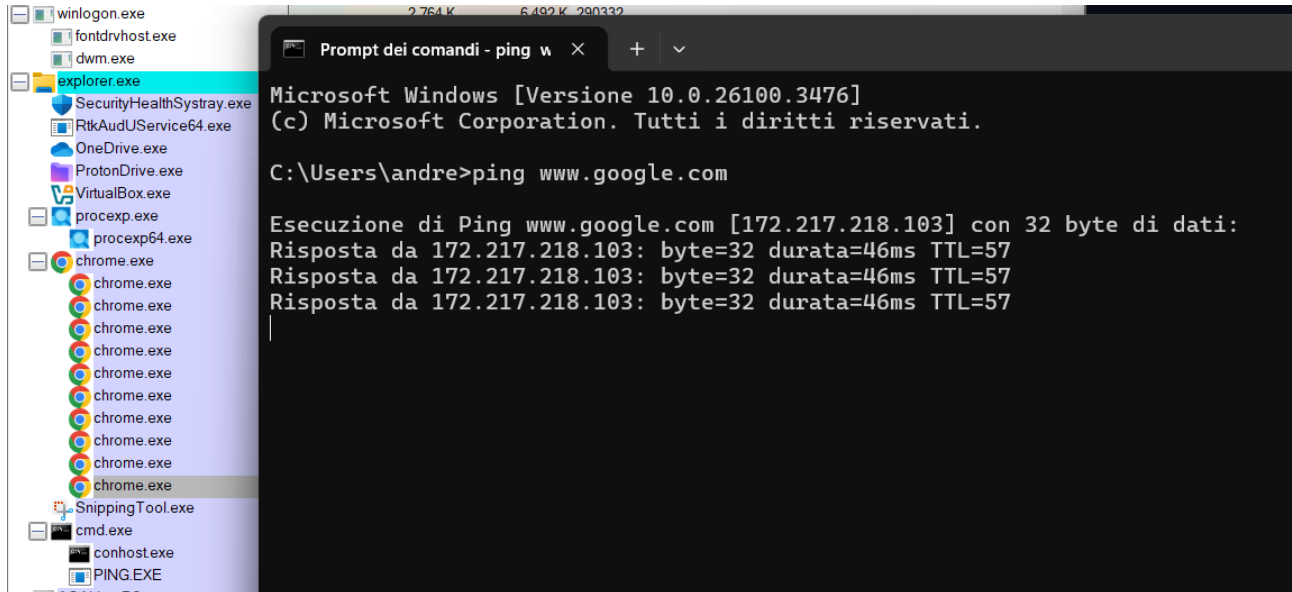
Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
lsass.exe		14.120 K	17.808 K	1136	Local Security Authority Proc...	Microsoft Corporation
fontdrvhost.exe		1.756 K	856 K	1312		
csrss.exe	< 0.01	3.160 K	4.744 K	323932		
winlogon.exe		2.764 K	6.728 K	290332		
fontdrvhost.exe		7.652 K	5.484 K	323812		
dwm.exe	1.64	247.280 K	150.852 K	307828		
explorer.exe	0.13	518.556 K	369.412 K	308056	Esplora risorse	Microsoft Corporation
SecurityHealthSystray.exe		1.992 K	3.868 K	287356	Windows Security notification ...	Microsoft Corporation
RtkAudUService64.exe	< 0.01	8.564 K	11.744 K	307534	Realtek HD Audio Universal...	Realtek Semiconductor
OneDrive.exe						Microsoft Corporation
ProtonDrive.exe						Proton AG
chrome.exe	< 0.01					Google LLC
chrome.exe	< 0.01					Google LLC
chrome.exe	< 0.01					Google LLC
chrome.exe	< 0.01					Google LLC
chrome.exe	< 0.01					Google LLC
chrome.exe	0.38					Google LLC
chrome.exe	< 0.01					Google LLC
chrome.exe	< 0.01	11.228 K	32.556 K	261812	Google Chrome	Google LLC
chrome.exe	0.38	221.024 K	230.628 K	315076	Google Chrome	Google LLC
chrome.exe		45.640 K	103.568 K	329148	Google Chrome	Google LLC
chrome.exe		13.952 K	30.812 K	328544	Google Chrome	Google LLC
VirtualBox.exe	< 0.01	91.232 K	123.092 K	325144	VirtualBox Manager	Oracle and/or its affiliates
procexp.exe		5.780 K	15.056 K	306552	Sysinternals Process Explorer	Sysinternals - www.sysinter...
procexp64.exe	0.25	291.316 K	325.872 K	325044	Sysinternals Process Explorer	Sysinternals - www.sysinter...
SnippingTool.exe	0.63	149.704 K	206.400 K	327076		
AQAUserPS.exe	< 0.01	6.984 K	12.232 K	270040		
ACCUserPS.exe		2.400 K	4.780 K	308208		
Discord.exe	< 0.01	113.040 K	80.760 K	302860	Discord	Discord Inc.



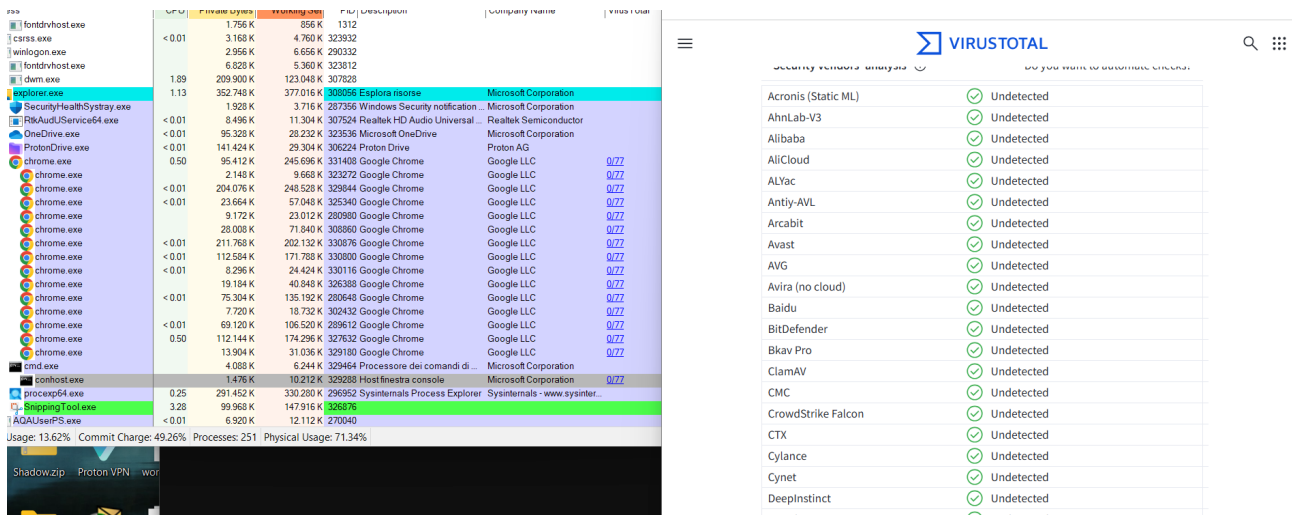
## PROCESSI FIGLI

Per questo esempio, apriamo sia CMD che Process Explorer come amministratori. Questo perchè su Windows 11 viene usato come terminale di default Windows Terminal, che su Process Explorer non elenca i processi figli.

Sulla CLI eseguiamo il ping e noteremo che creerà il processo figlio



Una bella comodità di Process Explorer di poter controllare se un processo è malevolo attraverso la verifica del processo con VirusTotal.com



## THREADS DEL PROCESSO conhost.exe

conhost.exe:312952 Properties

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

Count: 6

TID	CPU	Cycles Delta	Suspend Count	Start Address
347092				conhost.exe+0x25fb0
336892				ntdll.dll!TpCallbackMayRunLong+0x15f0
344880				combase.dll!RoParameterizedTypeExtraGetTypeSig...
287480				ntdll.dll!TpCallbackMayRunLong+0x15f0
325312				ntdll.dll!TpCallbackMayRunLong+0x15f0
325500				conhost.exe+0x998d0

Thread ID: 347092 Stack Module

Start Time: 18:23:16 09/04/2025

State: Wait:UserRequest Base Priority: 8

Kernel Time: 0:00:00.031 Dynamic Priority: 9

User Time: 0:00:00.015 I/O Priority: Normal

Context Switches: 423 Memory Priority: 5

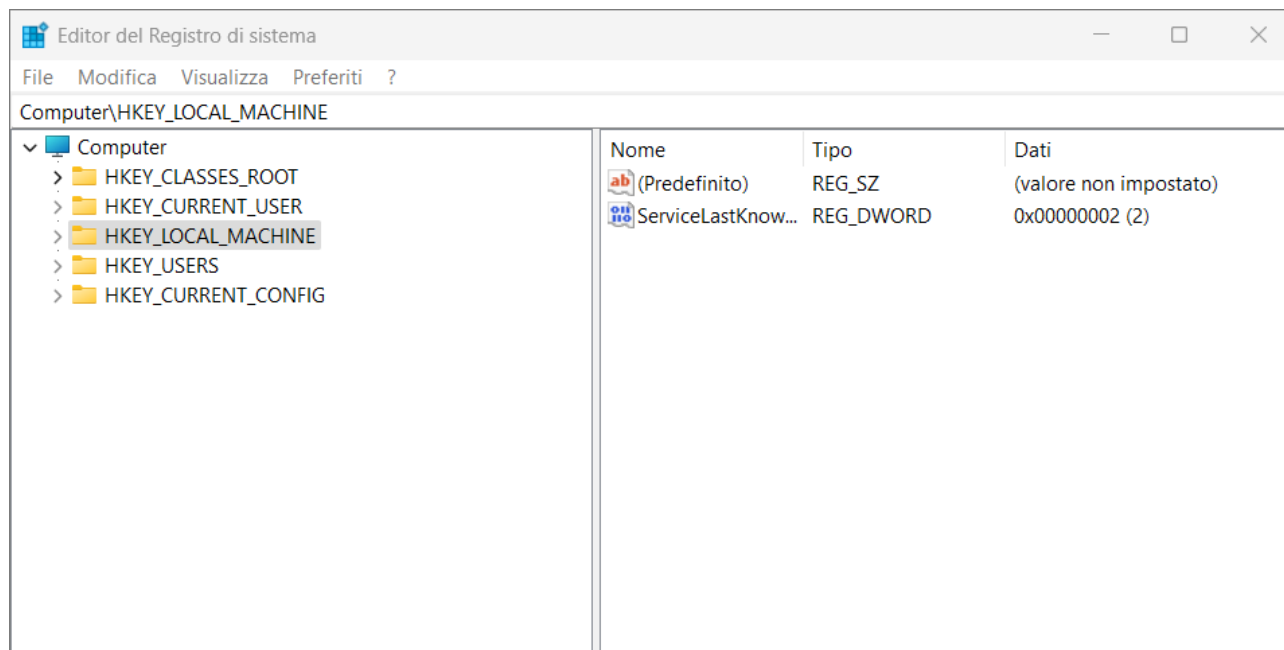
Cycles: 105.391.112 Ideal Processor: 6

Permissions Kill Suspend

OK Cancel

## NAVIGAZIONE ALLA CHIAVE EULA ACCEPTED

Per arrivare alla chiave EULA ACCEPTED bisogna cliccare su Start, digitare regedit e selezionare Editor del Registro di Sistema. Dopodiché selezionare HKEY\_LOCAL\_MACHINE > Software > Sysinternal > Process Explorer



Editor del Registro di sistema			
File Modifica Visualizza Preferiti ?			
Computer\HKEY_CURRENT_USER\Software\Sysinternals\Process Explorer			
	Nome	Tipo	Dati
> Acer	ColorSuspend	REG_DWORD	0x00808080 (8421504)
> Adobe	ColorSuspendDa...	REG_DWORD	0x001b1b1b (1776411)
> App Host Service	ConfirmKill	REG_DWORD	0x00000001 (1)
> appdatalow	DbgHelpPath	REG_SZ	C:\WINDOWS\SYSTEM32\db
> AppWork	DefaultDllProp...	REG_DWORD	0x00000000 (0)
> ChangeTracker	DefaultProcProp...	REG_DWORD	0x0000000d (13)
> Chromium	DefaultSysInfoPa...	REG_DWORD	0x00000000 (0)
> Cisco	Divider	REG_BINARY	00 00 00 00 00 00 e0 3f
> Cisco Spark Native	DllColumnCount	REG_DWORD	0x00000004 (4)
> Cisco Systems, Inc.	DllPropWindow...	REG_BINARY	2c 00 00 00 00 00 00 00 00 00
> Classes	DllSortColumn	REG_DWORD	0x00000000 (0)
> Discord	DllSortDirection	REG_DWORD	0x00000001 (1)
> ej-technologies	ETWstandardUse...	REG_DWORD	0x00000000 (0)
> Google	EulaAccepted	REG_DWORD	0x00000001 (1)
> Host App Service	FindWindowplac...	REG_BINARY	2c 00 00 00 00 00 00 00 00 00
> IM Providers	FormatloBytes	REG_DWORD	0x00000001 (1)
> JavaSoft	GpuNodeUsage...	REG_DWORD	0x00000001 (1)
> Microsoft	GpuNodeUsage...	REG_DWORD	0x00000000 (0)
> Mozilla	HandleColumnC...	REG_DWORD	0x00000002 (2)
> Netscape	HandleSortColu...	REG_DWORD	0x00000000 (0)
> ODBC	HandleSortDirec...	REG_DWORD	0x00000001 (1)
> OEM	HideWhenMinim...	REG_DWORD	0x00000000 (0)
> OpenOffice	HighlightDelProc	REG_DWORD	0x00000001 (1)
> Oracle	HighlightDuration	REG_DWORD	0x000003e8 (1000)
> Policies	HighlightImmers...	REG_DWORD	0x00000001 (1)
> Proton	HighlightJobs	REG_DWORD	0x00000000 (0)
> Python	HighlightNetPro...	REG_DWORD	0x00000000 (0)
> QtProject	HighlightNewProc	REG_DWORD	0x00000001 (1)
> Realtek	HighlightOwnPr...	REG_DWORD	0x00000001 (1)
> RegisteredApplications	HighlightPacked	REG_DWORD	0x00000001 (1)
> SyncEngines	HighlightProtect...	REG_DWORD	0x00000000 (0)
> Sysinternals			
> Process Explorer			
> WebEx			
> Wine			

Una volta individuata la chiave, cliccando due volte sulla stessa sarà possibile modificarla. In questo caso il valore dei dati che troviamo è 1, ciò vuol dire che l'EULA è stata accettata dall'Utente. Andando a sostituire il valore 1 con 0 sarà come non aver accettato l'EULA, nonostante avessimo già utilizzato il programma.

