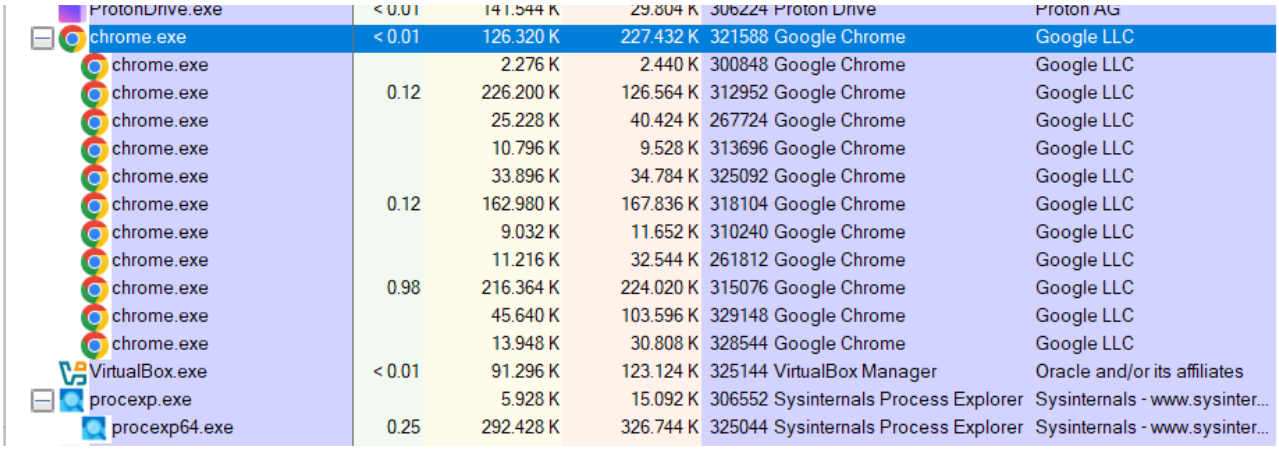
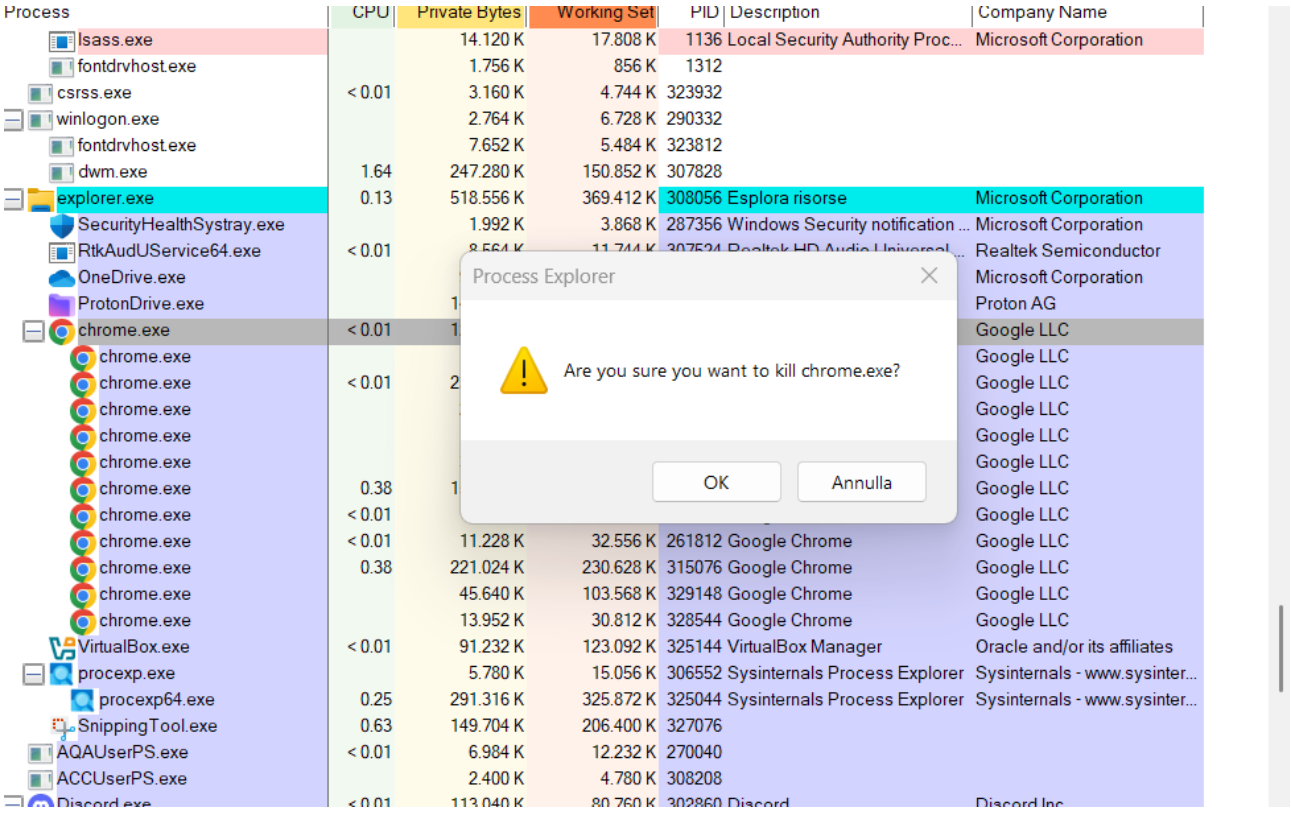
Esplorazione di Processi, Thread, Handle e Registro di Windows

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.

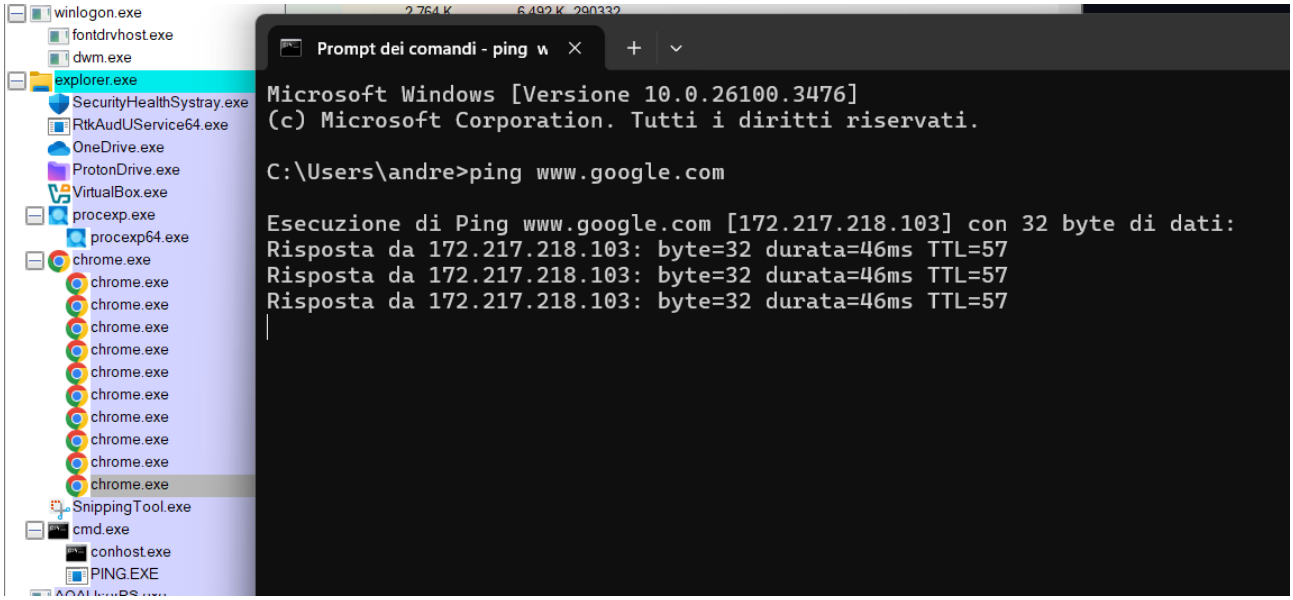
È possibile terminare il processo, in questo caso di Google Chrome, direttamente in Process Explorer. Per farlo, fare clic con il pulsante destro del mouse sul processo identificato e selezionare l'opzione "Kill Process". Confermare l'operazione cliccando su "OK" nella finestra di dialogo che



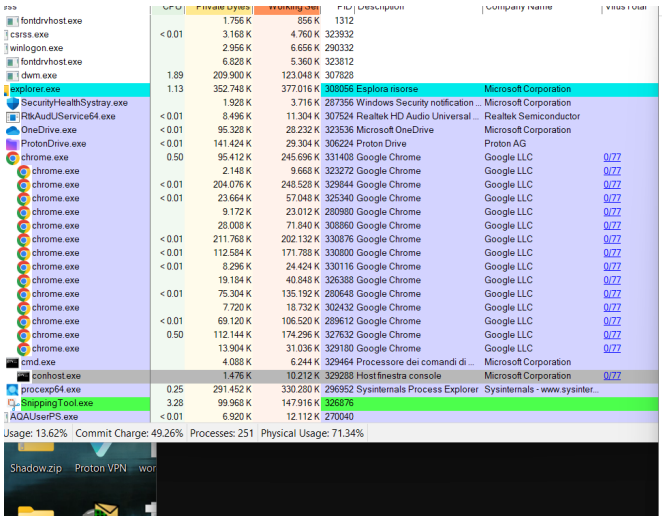


PROCESSI FIGLI

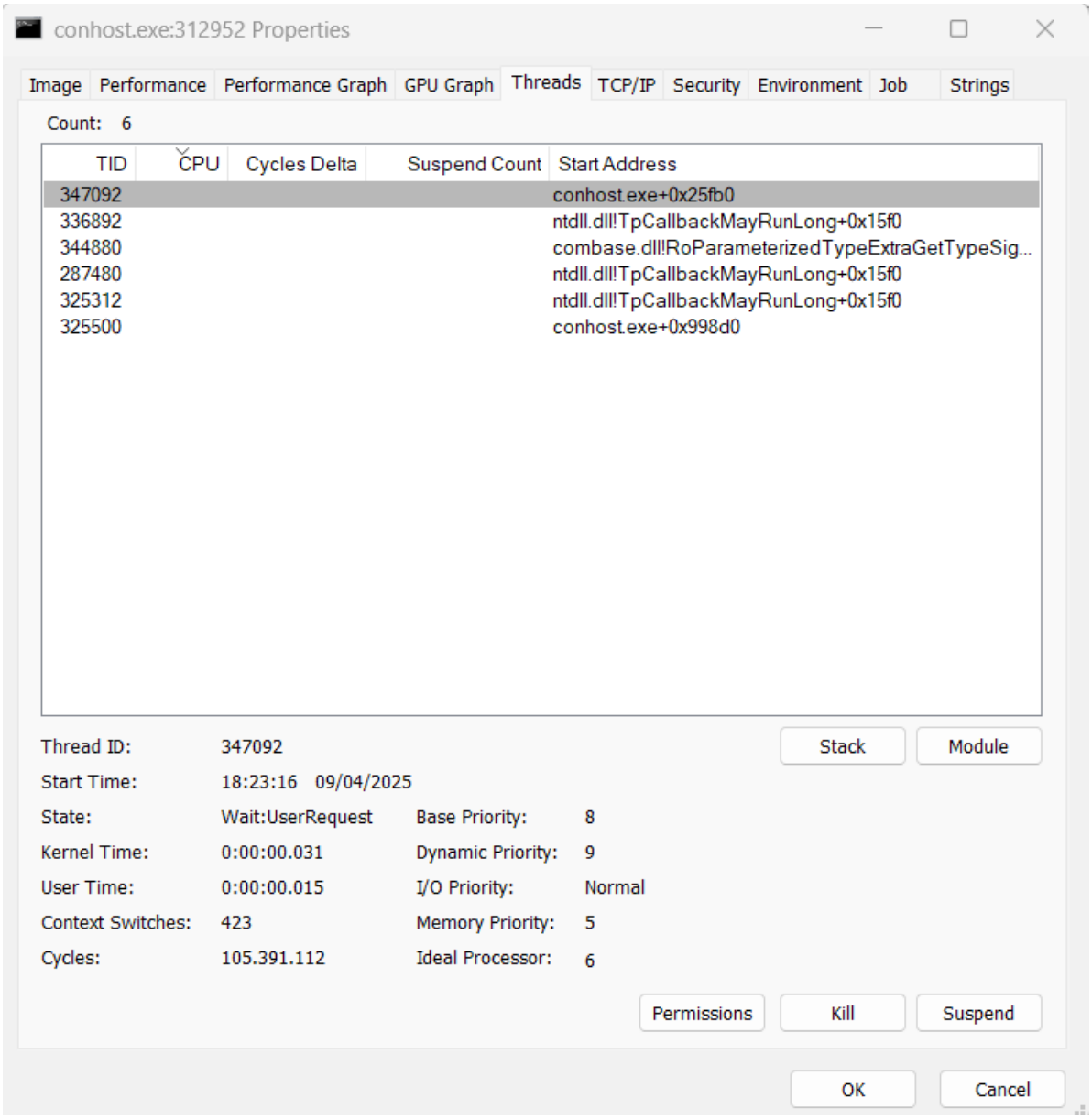
Per questo esempio, apriamo sia CMD che Process Explorer come amministratori. Questo perchè su Windows 11 viene usato come terminale di default Windows Terminal, che su Process Explorer non elenca i processi figli.
Sulla CLI eseguiamo il ping e noteremo che creerà il processo figlio



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

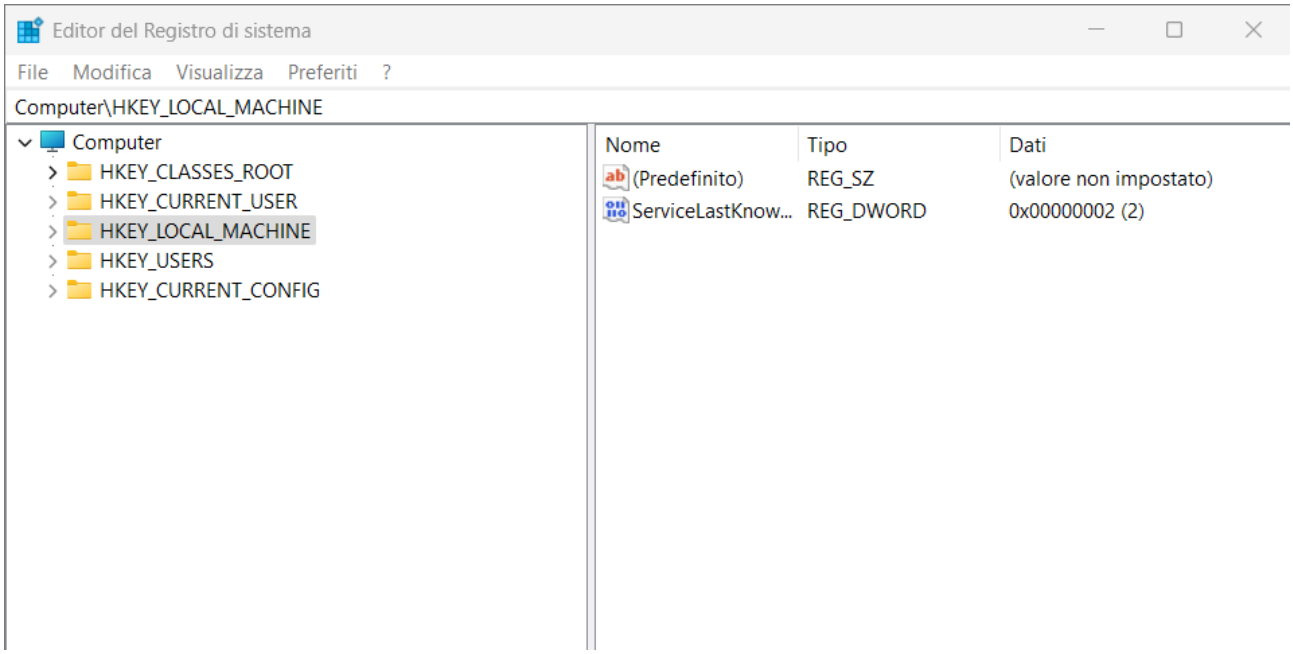


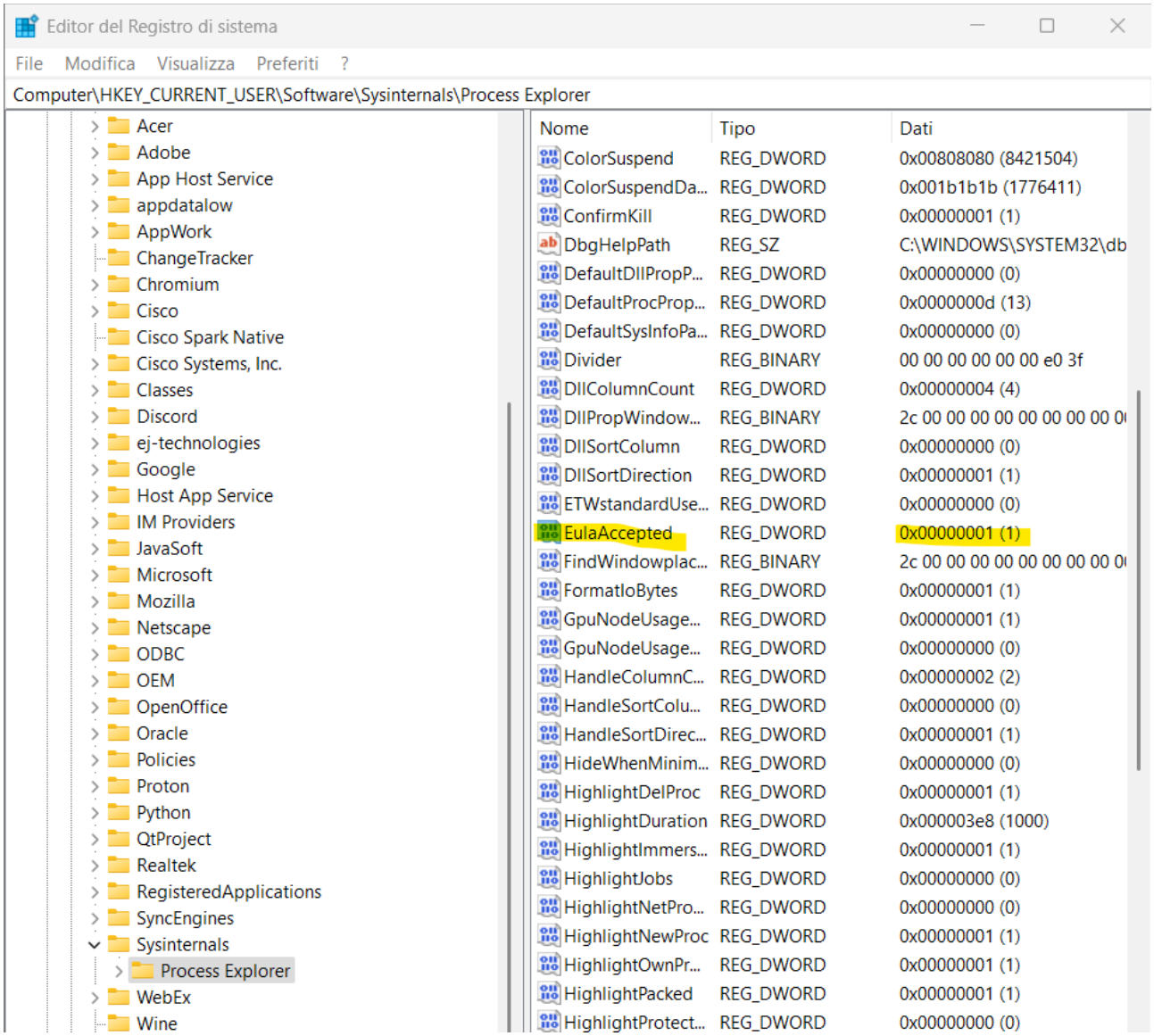
THREADS DEL PROCESSO conhost.exe



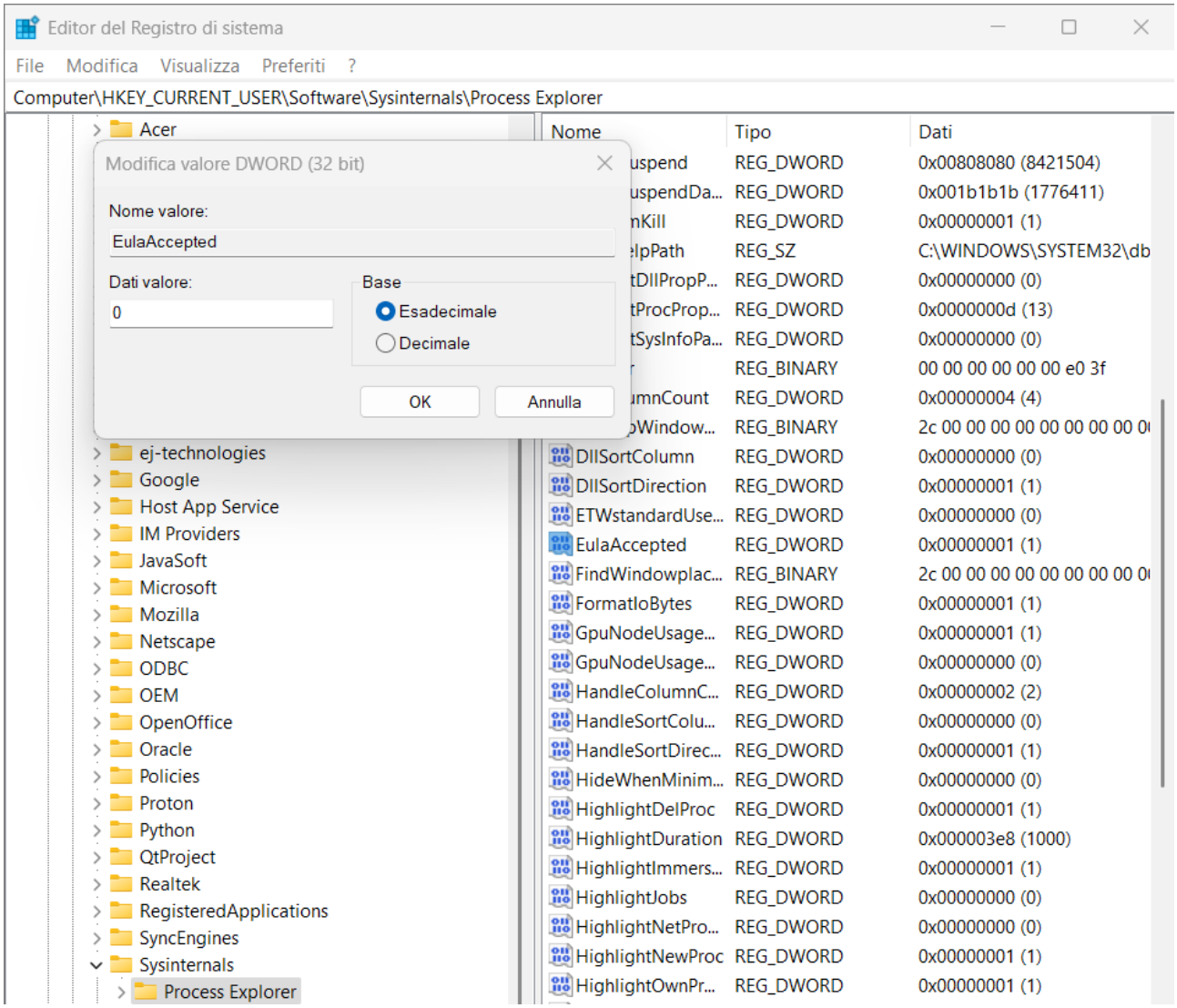
NAVIGAZIONE ALLA CHIAVE EULA ACCEPTED

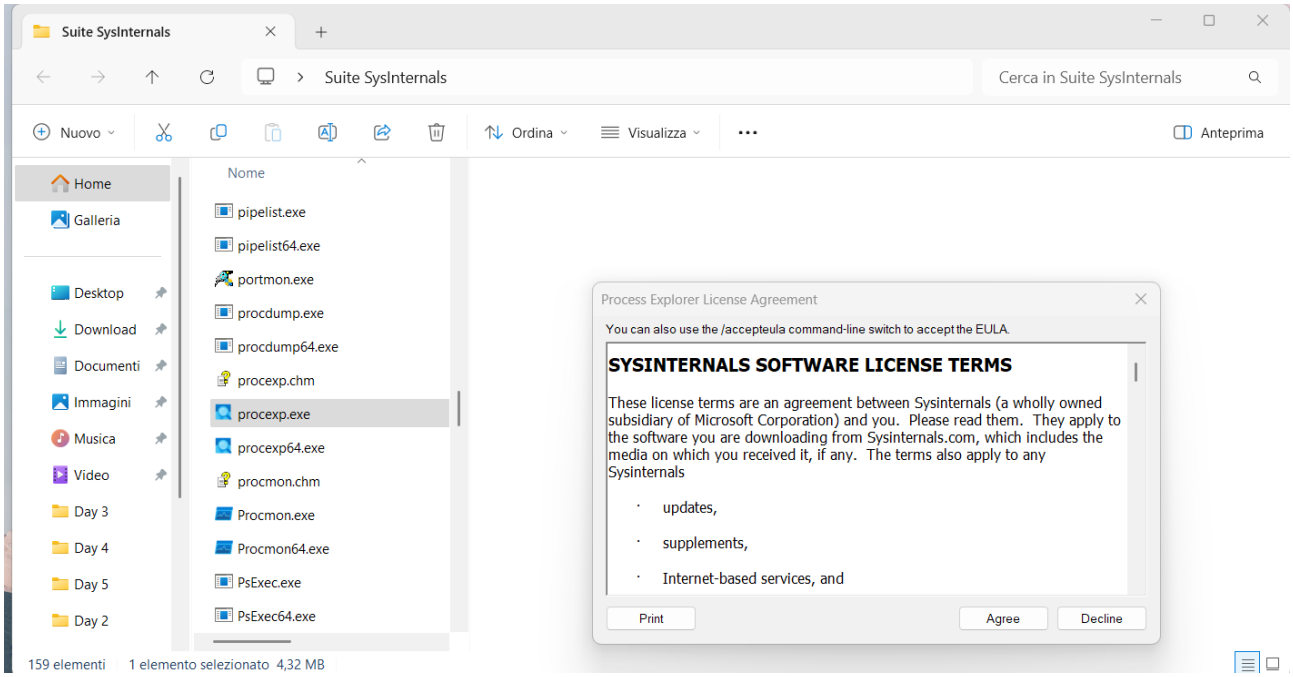
Per arrivare alla chiave EULA ACCEPTED bisogna cliccare su Start, digitare regedit e selezionare Editor del Registro di Sistema. Dopodiche selezionare HKEY_LOCAL_MACHINE > Software > Sysinternal > Process Explorer




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

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.




Suite SysInternals
Cerca in Suite SysInternals
Nuovo
Ordina
Visualizza
Anteprima
Home
Galleria
Desktop
Download
Documenti
Immagini
Musica
Video
Day 3
Day 4
Day 5
Day 2
Nome
pipelist.exe
pipelist64.exe
portmon.exe
procdump.exe
procdump64.exe
procexp.chm
procexp.exe
procexp64.exe
procmon.chm
Procmon.exe
Procmon64.exe
PsExec.exe
PsExec64.exe
159 elementi
1 elemento selezionato 4,32 MB
Process Explorer License Agreement
You can also use the /accepteula command-line switch to accept the EULA.
SYSINTERNALS SOFTWARE LICENSE TERMS
These license terms are an agreement between Sysinternals (a wholly owned subsidiary of Microsoft Corporation) and you. Please read them. They apply to the software you are downloading from Sysinternals.com, which includes the media on which you received it, if any. The terms also apply to any Sysinternals
updates,
supplements,
Internet-based services, and
Print
Agree
Decline