

PRATICA 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.

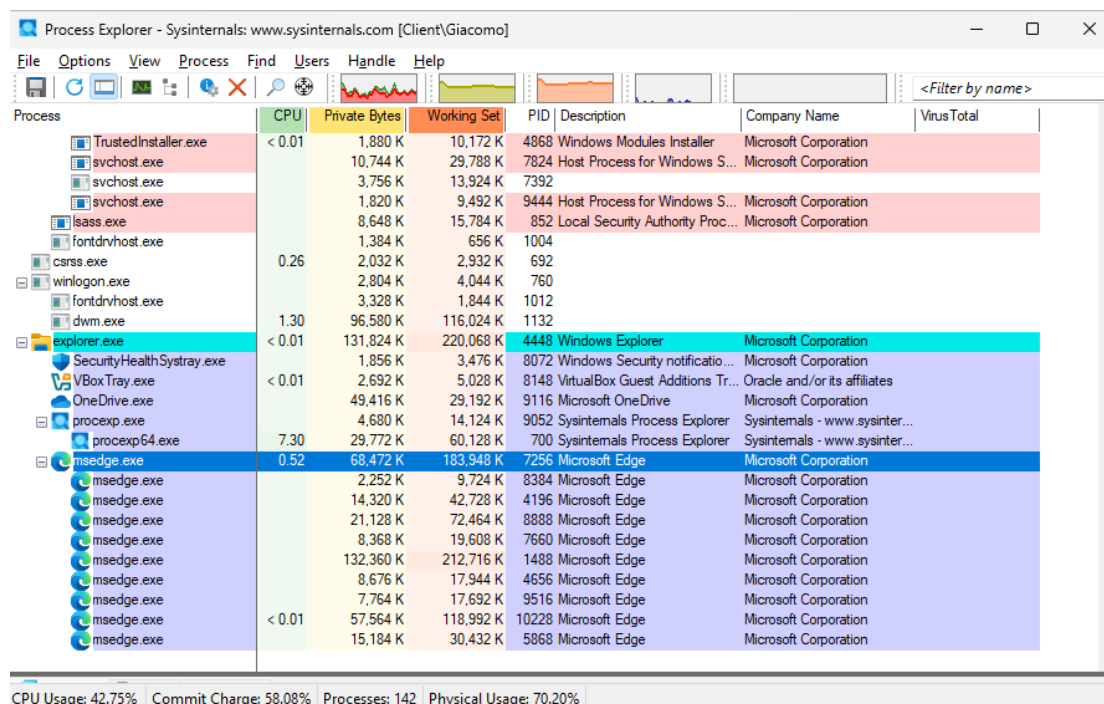
- Parte 1: Esplorazione dei Processi
- Parte 2: Esplorazione di Thread e Handle
- Parte 3: Esplorazione del Registro di Windows

Risorse Richieste

- 1 PC Windows con accesso a internet

Esplorare un processo attivo

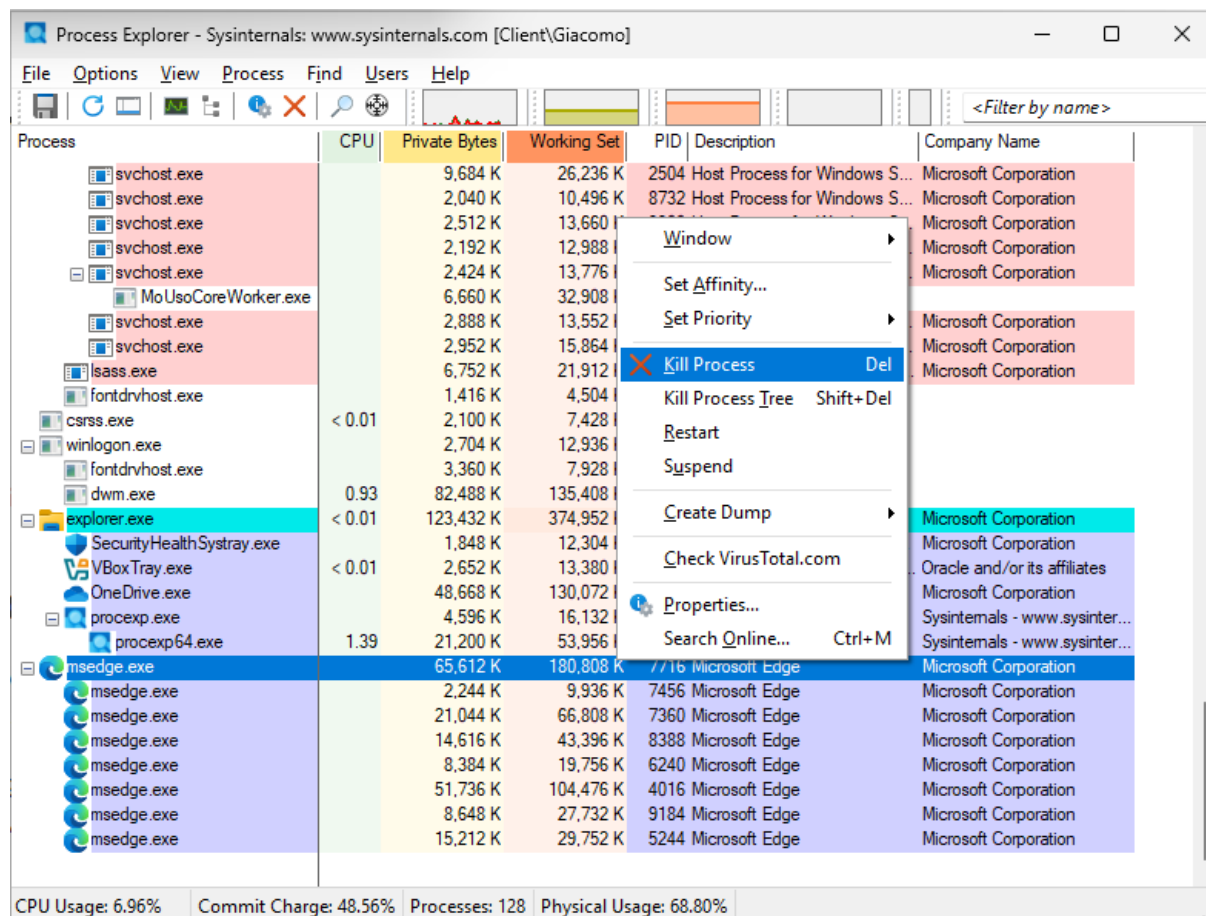
Dopo aver scaricato la **Sysinternals Suite** ed eseguito **procxp.exe**, ho utilizzato la funzione **Find Window's Process** trascinando la relativa icona sulla finestra del browser web aperta, al fine di identificarne il processo associato.



Process	CPU	Private Bytes	Working Set	PID	Description	Company Name	VirusTotal
TrustedInstaller.exe	< 0.01	1,880 K	10,172 K	4868	Windows Modules Installer	Microsoft Corporation	
svchost.exe		10,744 K	29,788 K	7824	Host Process for Windows S...	Microsoft Corporation	
svchost.exe		3,756 K	13,924 K	7392			
svchost.exe		1,820 K	9,492 K	9444	Host Process for Windows S...	Microsoft Corporation	
lsass.exe		8,648 K	15,784 K	852	Local Security Authority Proc...	Microsoft Corporation	
fontdrvhost.exe		1,384 K	656 K	1004			
csrss.exe	0.26	2,032 K	2,932 K	692			
winlogon.exe		2,804 K	4,044 K	760			
fontdrvhost.exe		3,328 K	1,844 K	1012			
dwm.exe	1.30	96,580 K	116,024 K	1132			
explorer.exe	< 0.01	131,824 K	220,068 K	4448	Windows Explorer	Microsoft Corporation	
SecurityHealthSystray.exe		1,856 K	3,476 K	8072	Windows Security notificatio...	Microsoft Corporation	
VBBoxTray.exe	< 0.01	2,692 K	5,028 K	8148	VirtualBox Guest Additions Tr...	Oracle and/or its affiliates	
OneDrive.exe		49,416 K	29,192 K	9116	Microsoft OneDrive	Microsoft Corporation	
procxp.exe		4,680 K	14,124 K	9052	Sysinternals Process Explorer	Sysinternals - www.sysinter...	
procxp64.exe	7.30	29,772 K	60,128 K	700	Sysinternals Process Explorer	Sysinternals - www.sysinter...	
msedge.exe	0.52	68,472 K	183,948 K	7256	Microsoft Edge	Microsoft Corporation	
msedge.exe		2,252 K	9,724 K	8384	Microsoft Edge	Microsoft Corporation	
msedge.exe		14,320 K	42,728 K	4196	Microsoft Edge	Microsoft Corporation	
msedge.exe		21,128 K	72,464 K	8888	Microsoft Edge	Microsoft Corporation	
msedge.exe		8,368 K	19,608 K	7660	Microsoft Edge	Microsoft Corporation	
msedge.exe		132,360 K	212,716 K	1488	Microsoft Edge	Microsoft Corporation	
msedge.exe		8,676 K	17,944 K	4656	Microsoft Edge	Microsoft Corporation	
msedge.exe		7,764 K	17,692 K	9516	Microsoft Edge	Microsoft Corporation	
msedge.exe	< 0.01	57,564 K	118,992 K	10228	Microsoft Edge	Microsoft Corporation	
msedge.exe		15,184 K	30,432 K	5868	Microsoft Edge	Microsoft Corporation	

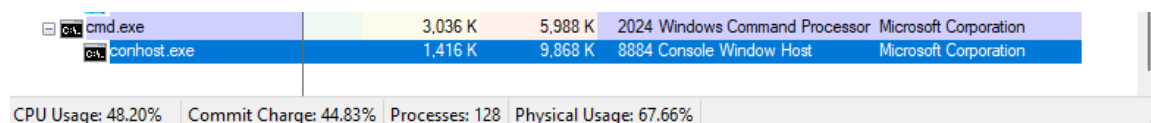
CPU Usage: 42.75% | Commit Charge: 58.08% | Processes: 142 | Physical Usage: 70.20%

Dopo aver individuato il processo corrispondente, ho cliccato con il tasto destro su di esso e selezionato il comando **Kill Process**. La finestra del browser web si è immediatamente chiusa: il programma è stato terminato.

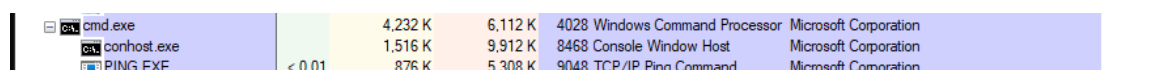


Avviare un altro processo

Dopo aver avviato il processo **cmd.exe**, ne ho verificato l'identità trascinando l'icona *Find Window's Process* sulla relativa finestra.

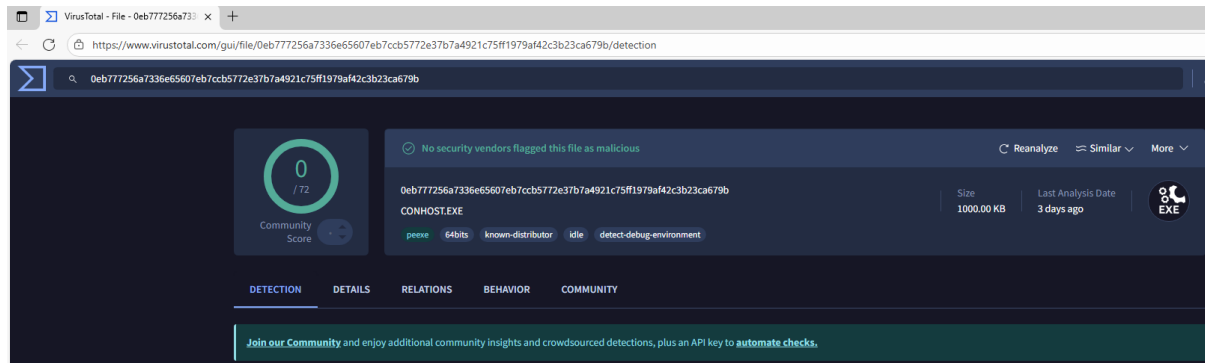


Ritornando alla finestra di **cmd.exe**, ho eseguito un comando di *ping* verso il DNS di Google (8.8.8.8), osservando in parallelo l'attività del processo tramite **Process Explorer**:

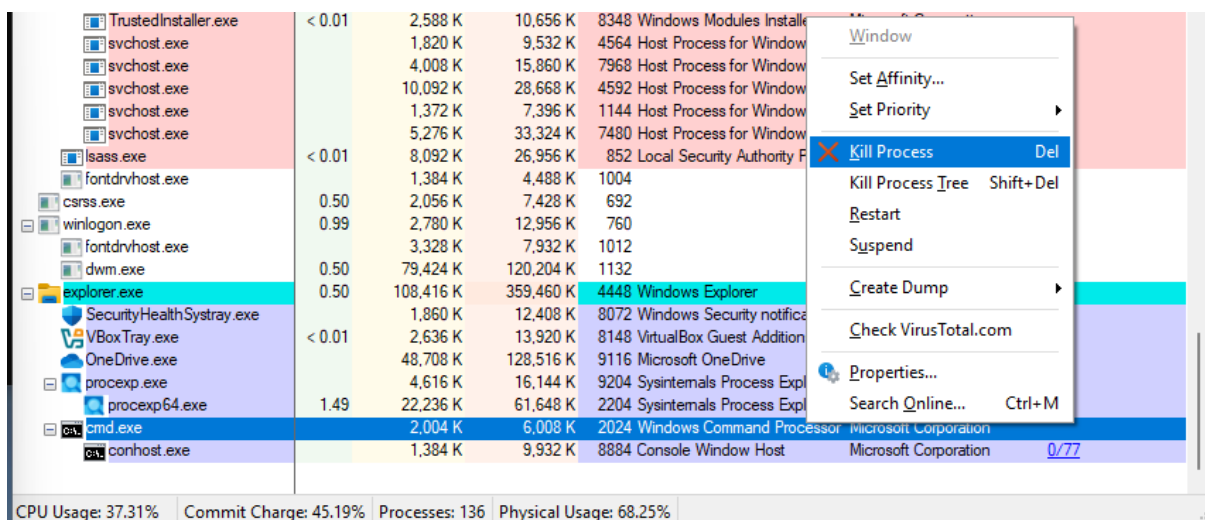


Durante l'esecuzione del comando *ping*, nel **Process Explorer** appare un nuovo processo denominato **PING.EXE**, che resta attivo per tutta la durata dell'operazione. Al termine, il processo si chiude autonomamente.

Tramite **Process Manager**, abbiamo selezionato il processo **conhost.exe** e avviato la verifica tramite **VirusTotal**. L'analisi dell'hash ha coinvolto 72 motori antivirus, nessuno dei quali ha rilevato elementi malevoli: il file risulta pulito.



Dopo le varie analisi, ritorno su **Process Manager** per “Killare” il processo tramite il comando **Kill Process**

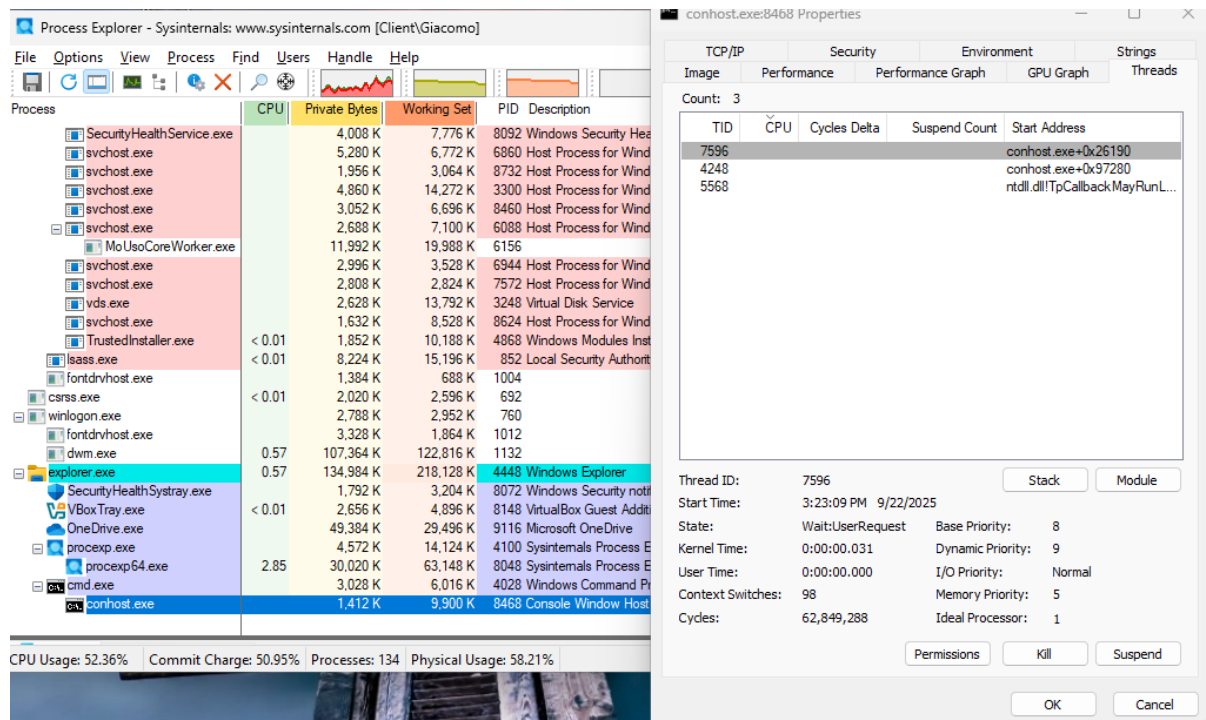


Questo comporta, ovviamente, anche la terminazione del processo “figlio” **conhost.exe**

Esplorazione di Thread e Handle

Esplorare i thread

Per visualizzare i **thread** in **Process Explorer**, è sufficiente aprire le **proprietà** del processo desiderato e selezionare la scheda **Threads**.



Oltre alla scheda **Threads**, la finestra delle **proprietà** di un processo in **Process Explorer** offre numerose informazioni dettagliate, tra cui:

- **Image** Mostra le informazioni fondamentali sul processo, tra cui:
 - Percorso completo dell'eseguibile
 - Riga di comando utilizzata per l'avvio
 - Orario di avvio
 - Nome dell'utente che ha avviato il processo
- **Performance** Visualizza grafici in tempo reale sull'utilizzo di CPU e memoria. Include:
 - Tempo di esecuzione in modalità kernel e utente
 - Byte privati allocati
 - Indicatori utili per identificare processi ad alto consumo di risorse
- **Performance Graph** Offre una rappresentazione grafica dettagliata della cronologia di utilizzo di:
 - CPU
 - Memoria
 - Input/Output

- **GPU Graph** Se presente una GPU nel sistema, questa scheda mostra:
 - Utilizzo della GPU da parte del processo
 - Identificazione di applicazioni che sfruttano intensivamente la scheda grafica
- **Threads** Elenca tutti i thread attivi nel processo, con dettagli su:
 - ID del thread
 - Utilizzo della CPU
 - Stato operativo:

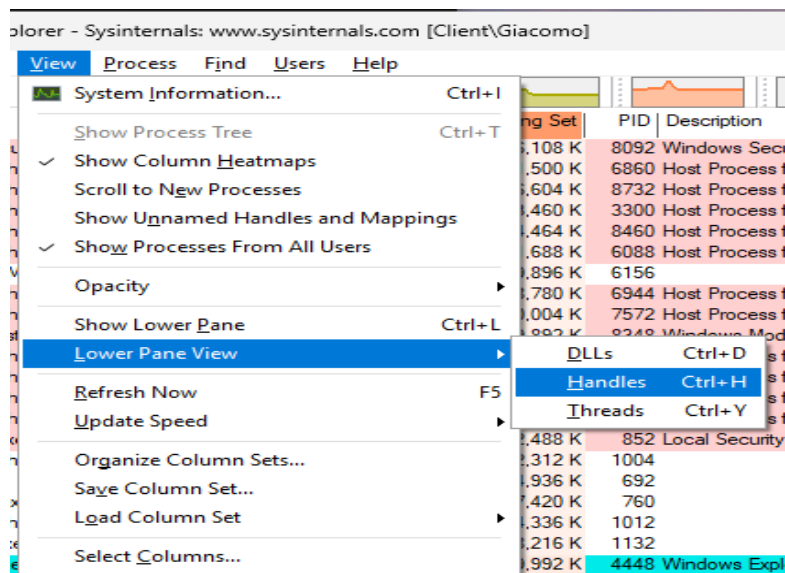
Utile per analizzare il comportamento del processo a livello di micro-esecuzione.
- **TCP/IP** Mostra le connessioni di rete aperte dal processo, inclusi:
 - Indirizzi locali e remoti
 - Porte utilizzate
 - Stato delle connessioni:

Fondamentale per investigare attività di rete sospette o potenzialmente malevole.
- **Security** Visualizza le credenziali di sicurezza del processo, tra cui:
 - Permessi
 - Gruppi di appartenenza
 - Privilegi attivi:

Aiuta a comprendere il livello di autorizzazione con cui il processo opera.
- **Environment** Elenca tutte le variabili d'ambiente attive per il processo, ereditate o impostate.
- **Strings** Estrae le stringhe leggibili (ASCII e Unicode) dal file eseguibile e dalla memoria del processo. Può rivelare:
 - Nomi di file
 - URL
 - Messaggi di errore
 - Dati nascosti o diagnostici utili per l'analisi.

Esplorare gli handle

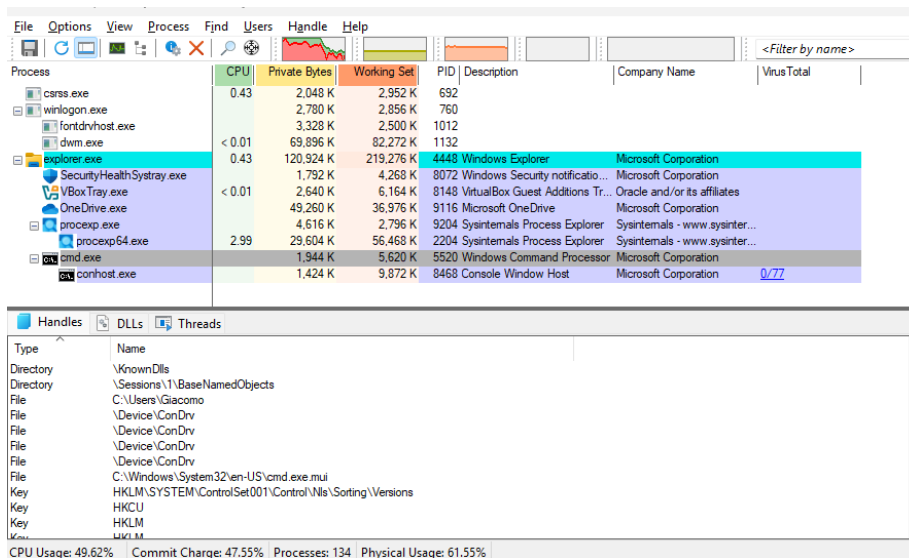
In **Process Explorer**, per visualizzare gli **handle** associati al processo **conhost.exe**, è sufficiente fare clic su **View (Visualizza) > Lower Pane View (Vista Riquadro Inferiore) > selezionare Handles**.



Basandoci sull'osservazione dello screen, gli **handle** visualizzati nel riquadro inferiore di **Process Explorer** rappresentano le risorse di sistema attualmente aperte o utilizzate dal processo selezionato **conhost.exe**.

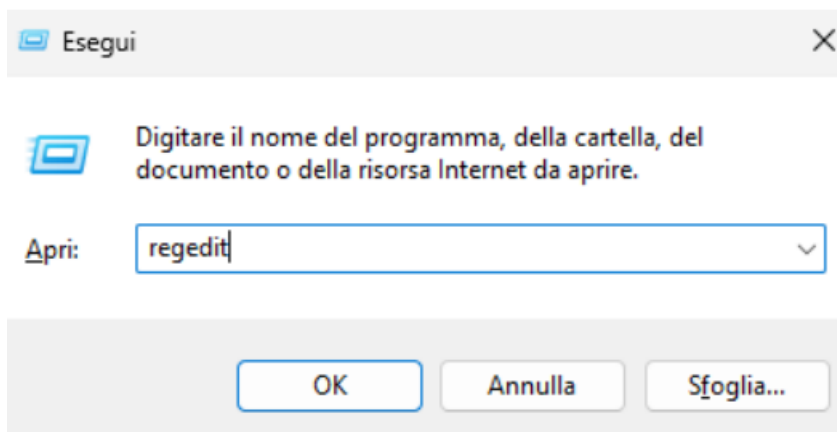
- Ogni **riga** nella colonna **Name** mostra il **percorso** o il **nome** della risorsa associata, come file, chiavi di registro, eventi, mutex o altri oggetti di sistema.
- La colonna **Type** indica la **tipologia** della risorsa, permettendo di distinguere tra oggetti come:
 - File → file aperti dal processo
 - Key → chiavi di registro
 - Event → eventi di sincronizzazione
 - Mutant → mutex (mutual exclusion objects)
 - Section → segmenti di memoria condivisa
 - WindowStation, Desktop, Token, ecc.

Questa vista è fondamentale per comprendere quali risorse il processo sta utilizzando e può aiutare nell'identificazione di comportamenti sospetti o non documentati.



Esplorazione del Registro di Windows

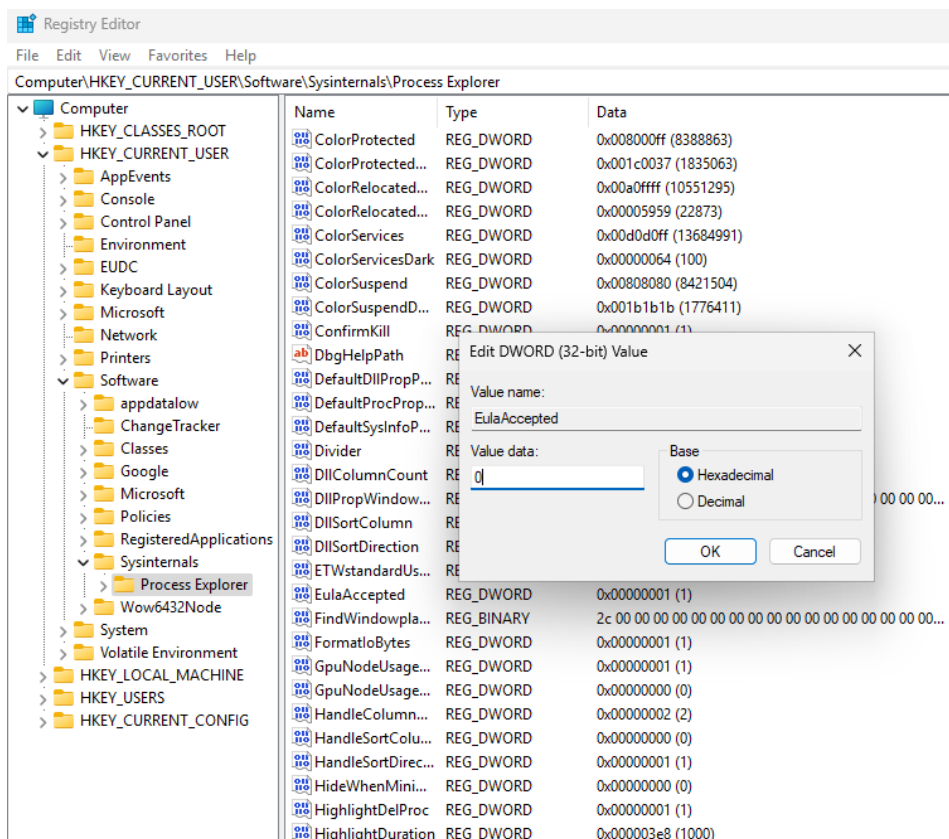
Dopo aver chiuso **Process Explorer**, premo **Win+R** e digito **regedit** per aprire l'**Editor del Registro di sistema** di Windows.



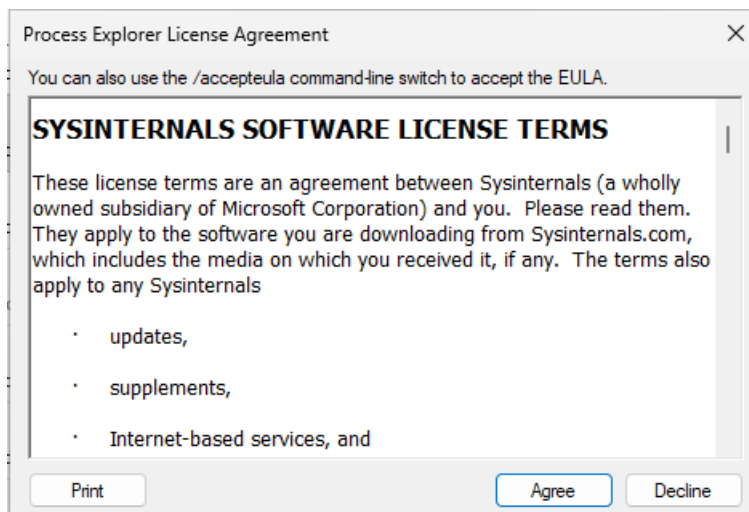
Mi sono spostato nel percorso:

HKEY_CURRENT_USER\Software\Sysinternals\Process Explorer

Qui ho individuato la voce **EulaAccepted**. Facendo doppio clic su di essa, si è aperta la finestra di modifica del valore **DWORD**. Ho verificato che il campo **Value data** fosse impostato su **1** in base **esadecimale**, confermando così che l'**EULA** di Process Explorer era già stata accettata.



In base alla traccia, ho modificato manualmente il valore della chiave **EulaAccepted** nel Registro di sistema, impostandolo a 0 per simulare la mancata accettazione dei termini di licenza. Successivamente, ho riavviato **Process Explorer**: come previsto, all'avvio è ricomparsa la finestra con i termini della **EULA**, che ho dovuto riconfermare. Una volta accettati, il valore della chiave **EulaAccepted** è stato automaticamente riportato a 1, indicando l'avvenuta accettazione.



Conclusione

In questo esercizio ho esplorato in modo approfondito il comportamento e le funzionalità di **Process Explorer**, integrando osservazioni pratiche con interventi diretti sul **Registro di sistema**. Dopo aver scaricato e avviato **procexp.exe**, ho utilizzato la funzione *Find Window's Process* per identificare processi attivi come il browser web e **cmd.exe**, osservando come ogni processo si manifesta e si comporta all'interno dell'interfaccia di Process Explorer.

Ho analizzato l'effetto del comando **Kill Process**, verificando la chiusura immediata del processo selezionato e dei suoi eventuali processi figli, come **conhost.exe**. Durante l'esecuzione di comandi come `ping 8.8.8.8`, ho monitorato la comparsa temporanea del processo **PING.EXE**, che si autotermina al termine dell'operazione.

Attraverso la finestra delle **proprietà** dei processi, ho esplorato schede informative come *Image*, *Performance*, *Threads*, *TCP/IP*, *Security*, *Environment*, *Strings*, e altre, comprendendo il valore diagnostico di ciascuna. Ho anche attivato la **Lower Pane View** per visualizzare gli **handle** associati ai processi, osservando le risorse di sistema a cui ogni processo accede.

Infine, ho interagito direttamente con il **Registro di sistema**, modificando la chiave `EulaAccepted` per simulare la mancata accettazione della licenza d'uso. Al riavvio di Process Explorer, ho verificato la riapparizione della finestra EULA e la successiva modifica automatica del valore a 1 una volta accettati i termini.