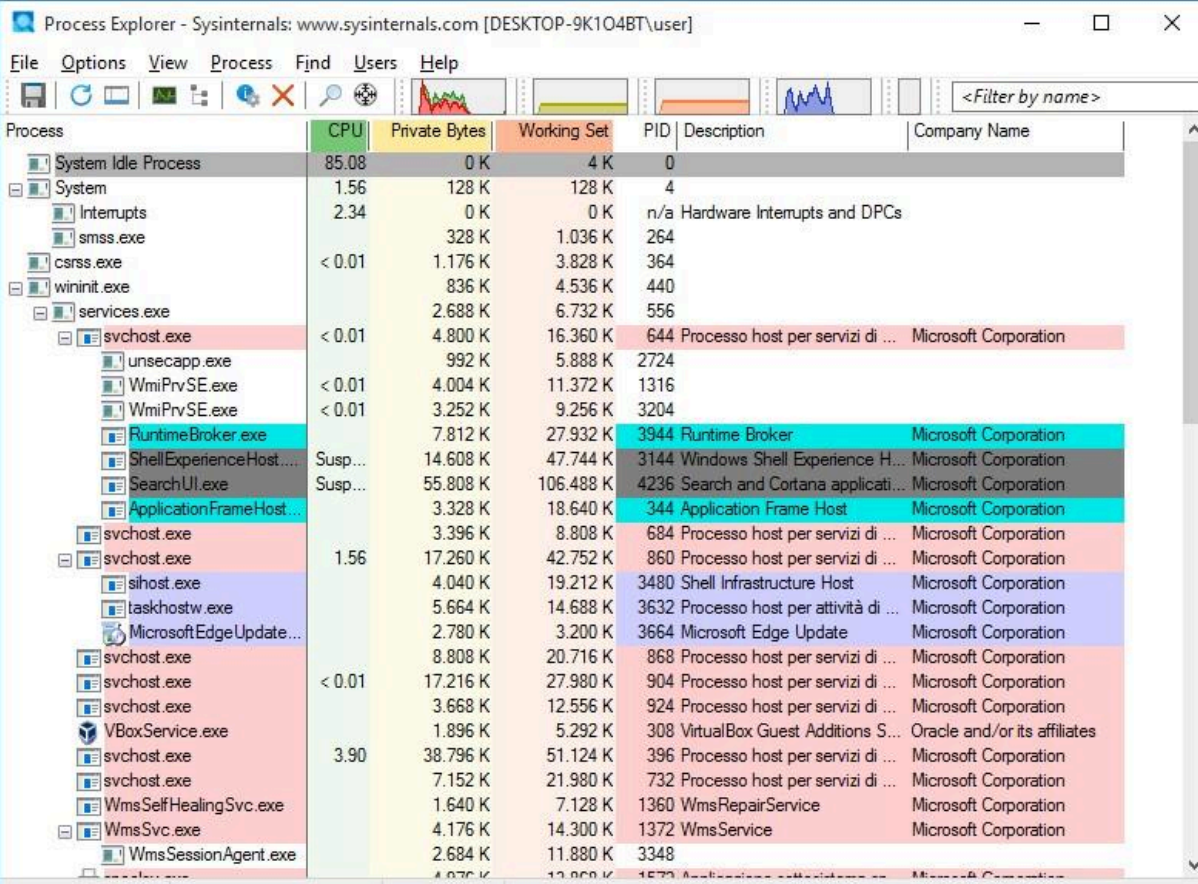


## S11 L2 - Laboratori giorno 1 – Cisco CyberOps

### PARTE 1

#### Esplorare un processo attivo

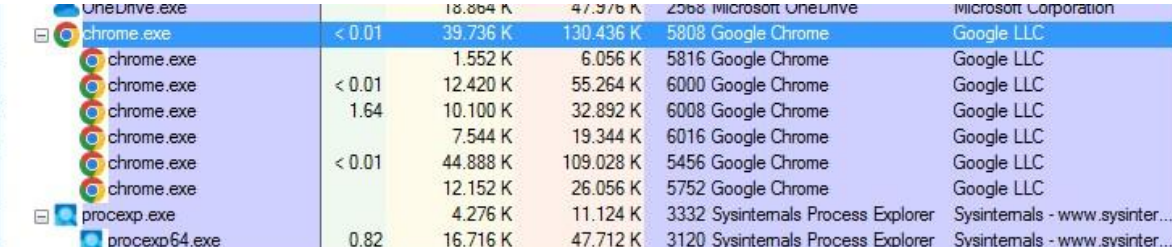
- Avvia il file **procexp.exe** e accetta il Contratto di licenza di Process Explorer.
- Una volta aperto Process Explorer, verrà visualizzato un elenco dei processi attualmente attivi.
- Per individuare il processo del browser Web aperto:
  - Trascina l'icona **Processo della finestra Trova** (che si trova nella barra degli strumenti di Process Explorer) all'interno della finestra del browser aperto.



Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
System Idle Process	85.08	0 K	4 K	0		
System	1.56	128 K	128 K	4		
Interrupts	2.34	0 K	0 K	n/a	Hardware Interrupts and DPCs	
smss.exe		328 K	1.036 K	264		
csrss.exe	< 0.01	1.176 K	3.828 K	364		
wininit.exe		836 K	4.536 K	440		
services.exe		2.688 K	6.732 K	556		
svchost.exe	< 0.01	4.800 K	16.360 K	644	Processo host per servizi di ...	Microsoft Corporation
unsecapp.exe		992 K	5.888 K	2724		
WmiPrivSE.exe	< 0.01	4.004 K	11.372 K	1316		
WmiPrivSE.exe	< 0.01	3.252 K	9.256 K	3204		
RuntimeBroker.exe		7.812 K	27.932 K	3944	Runtime Broker	Microsoft Corporation
ShellExperienceHost.exe	Susp...	14.608 K	47.744 K	3144	Windows Shell Experience H...	Microsoft Corporation
SearchUI.exe	Susp...	55.808 K	106.488 K	4236	Search and Cortana applicati...	Microsoft Corporation
ApplicationFrameHost.exe		3.328 K	18.640 K	344	Application Frame Host	Microsoft Corporation
svchost.exe		3.396 K	8.808 K	684	Processo host per servizi di ...	Microsoft Corporation
svchost.exe	1.56	17.260 K	42.752 K	860	Processo host per servizi di ...	Microsoft Corporation
sihost.exe		4.040 K	19.212 K	3480	Shell Infrastructure Host	Microsoft Corporation
taskhostw.exe		5.664 K	14.688 K	3632	Processo host per attività di ...	Microsoft Corporation
Microsoft Edge Update...		2.780 K	3.200 K	3664	Microsoft Edge Update	Microsoft Corporation
svchost.exe		8.808 K	20.716 K	868	Processo host per servizi di ...	Microsoft Corporation
svchost.exe	< 0.01	17.216 K	27.980 K	904	Processo host per servizi di ...	Microsoft Corporation
svchost.exe		3.668 K	12.556 K	924	Processo host per servizi di ...	Microsoft Corporation
VBService.exe		1.896 K	5.292 K	308	VirtualBox Guest Additions S...	Oracle and/or its affiliates
svchost.exe	3.90	38.796 K	51.124 K	396	Processo host per servizi di ...	Microsoft Corporation
svchost.exe		7.152 K	21.980 K	732	Processo host per servizi di ...	Microsoft Corporation
WmsSelfHealingSvc.exe		1.640 K	7.128 K	1360	WmsRepairService	Microsoft Corporation
WmsSvc.exe		4.176 K	14.300 K	1372	WmsService	Microsoft Corporation
WmsSessionAgent.exe		2.684 K	11.880 K	3348		

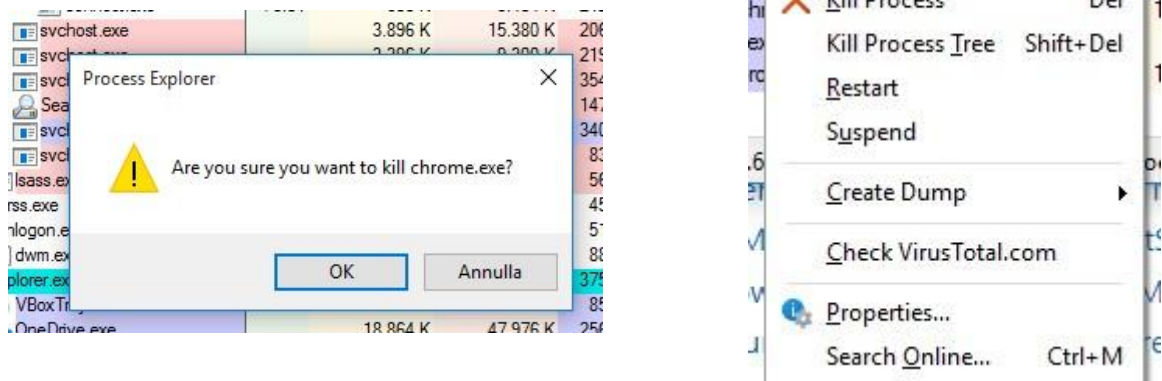
CPU Usage: 17.95% Commit Charge: 37.19% Processes: 71 Physical Usage: 43.26%

- Ad esempio, se stai usando Chrome, questo processo verrà evidenziato.

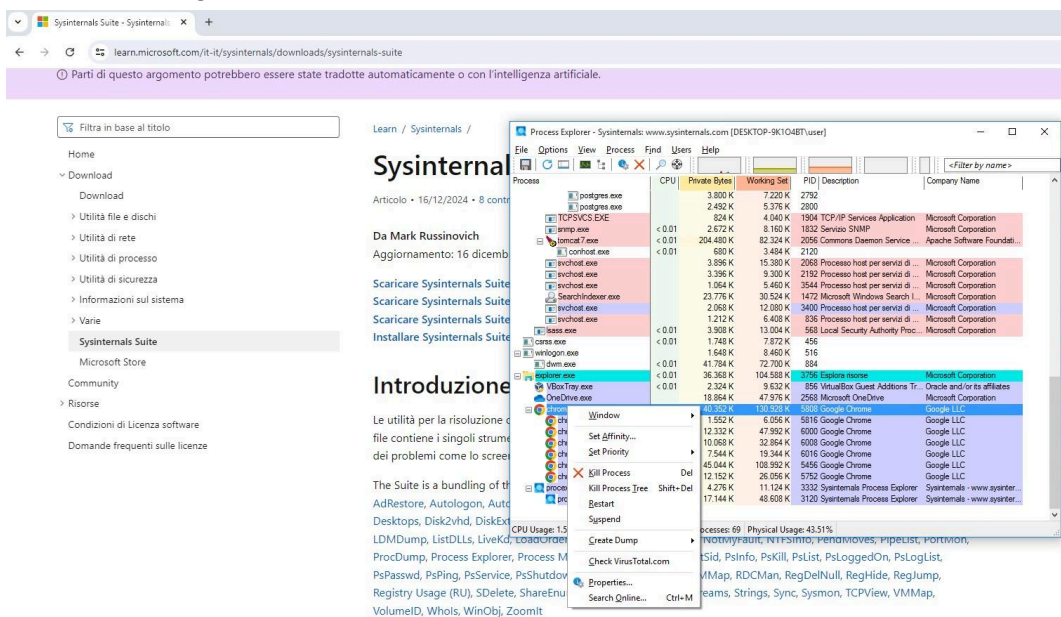


OneDrive.exe		18.864 K	47.376 K	2968	Microsoft OneDrive	Microsoft Corporation
chrome.exe	< 0.01	39.736 K	130.436 K	5808	Google Chrome	Google LLC
chrome.exe		1.552 K	6.056 K	5816	Google Chrome	Google LLC
chrome.exe	< 0.01	12.420 K	55.264 K	6000	Google Chrome	Google LLC
chrome.exe	1.64	10.100 K	32.892 K	6008	Google Chrome	Google LLC
chrome.exe		7.544 K	19.344 K	6016	Google Chrome	Google LLC
chrome.exe	< 0.01	44.888 K	109.028 K	5456	Google Chrome	Google LLC
chrome.exe		12.152 K	26.056 K	5752	Google Chrome	Google LLC
procexp.exe		4.276 K	11.124 K	3332	Sysinternals Process Explorer	Sysinternals - www.sysinter...
procexp64.exe	0.82	16.716 K	47.712 K	3120	Sysinternals Process Explorer	Sysinternals - www.sysinter...

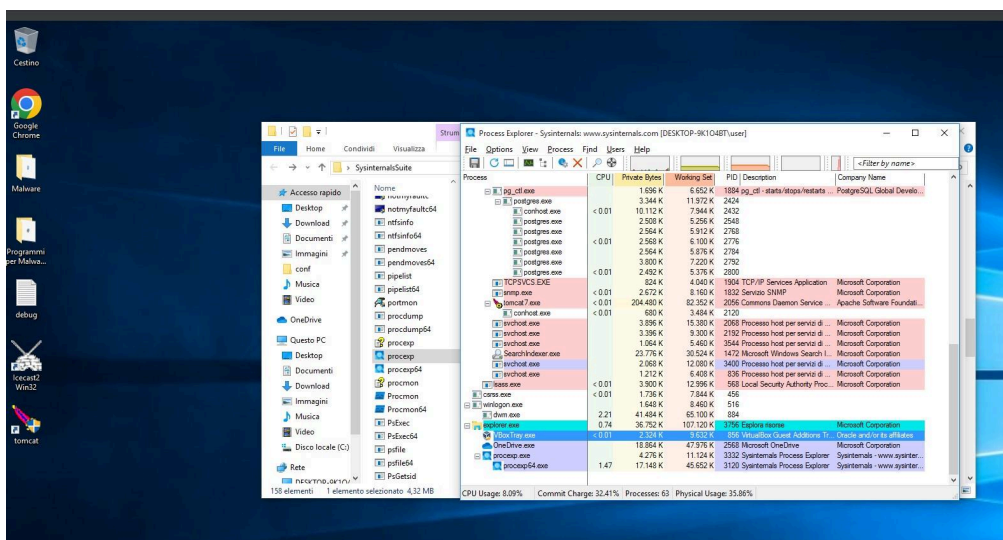
- Il processo Chrome può essere terminato in Process Explorer. Fai clic con il pulsante destro del mouse sul processo selezionato e seleziona **Kill Process**. Fai clic su **OK** per continuare.



Prima:



Dopo (Chromo si è chiuso):



## PARTE 2

### Passaggio 3: Avviare un nuovo processo

1. Apri un prompt dei comandi:
2. Usa l'icona "Trova processo" per individuare il processo del prompt dei comandi in Process Explorer.
  - Il processo associato sarà **cmd.exe**.
  - Esamina la relazione tra i processi:
    - **Padre:** explorer.exe
    - **Figlio:** conhost.exe
3. Dal prompt dei comandi, esegui il comando **ping** e osserva i cambiamenti nel processo **cmd.exe** in Process Explorer.  
Si osservano variazioni nell'attività del processo **cmd.exe**.

procexp64.exe	1.49	17.240 K	39.492 K	3120 Sysinternals Process Explorer	Sysinternals - www.sysinter..
cmd.exe		1.568 K	3.008 K	2316 Processore dei comandi di ...	Microsoft Corporation
conhost.exe	< 0.01	9.280 K	12.716 K	5340 Console Window Host	Microsoft Corporation
PING.EXE	< 0.01	720 K	3.464 K	5904 Comando Ping TCP/IP	Microsoft Corporation

## Parte 3: Esplorazione del Registro di sistema di Windows

Il Registro di sistema di Windows è un database gerarchico che archivia la maggior parte delle impostazioni di configurazione relative al sistema operativo e all'ambiente desktop.

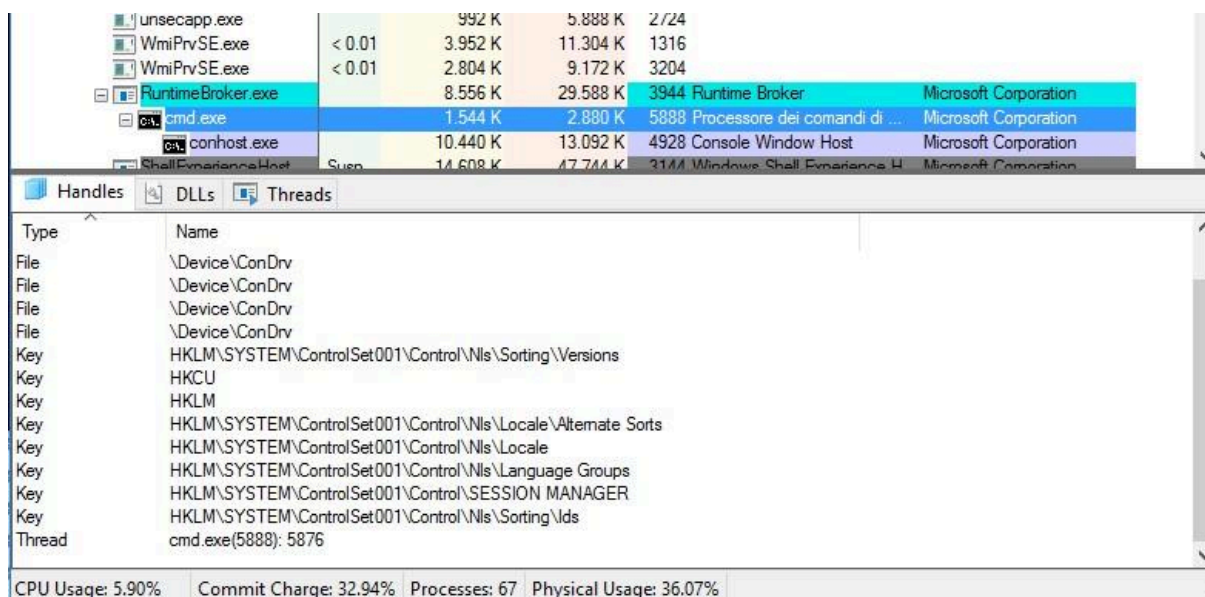
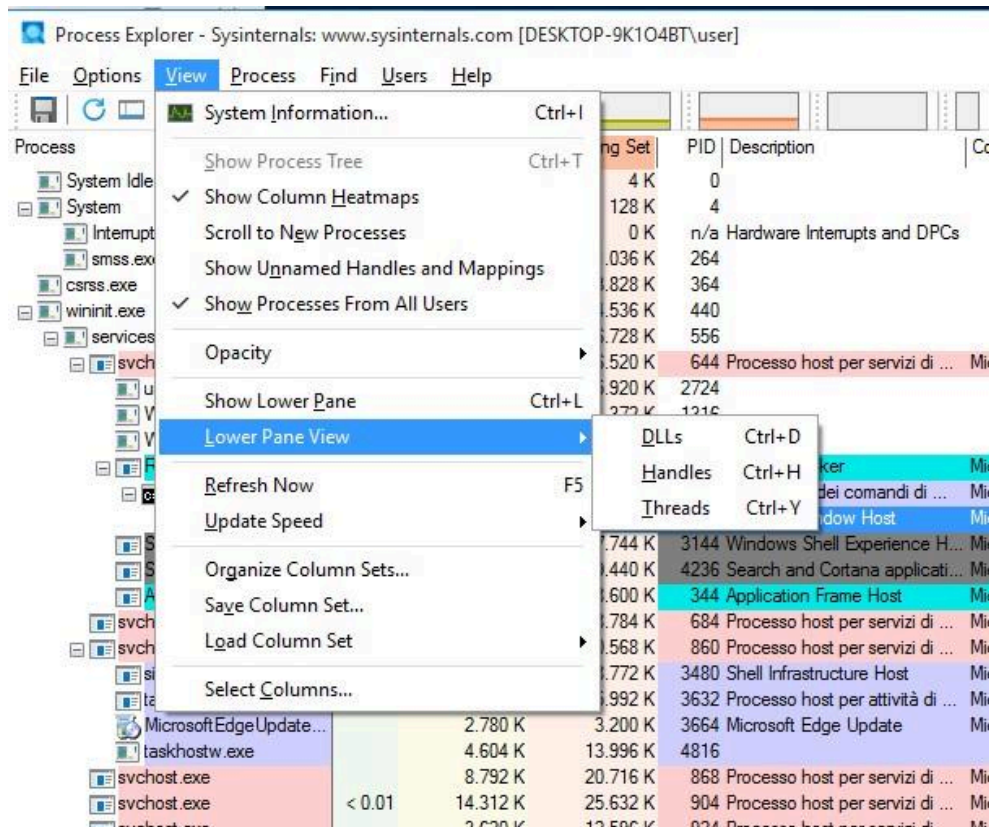
Per accedere al Registro di sistema di Windows:

1. Fai clic su **Start**.
2. Digita **regedit** nella barra di ricerca e seleziona **Editor del Registro di sistema**.



## Esplorare gli handle

1. In Process Explorer, attiva la **Visualizzazione riquadro inferiore**:
  - **Visualizza** → **Visualizzazione riquadro inferiore** → **Handle**.
2. Esamina gli handle associati al processo **conhost.exe**.

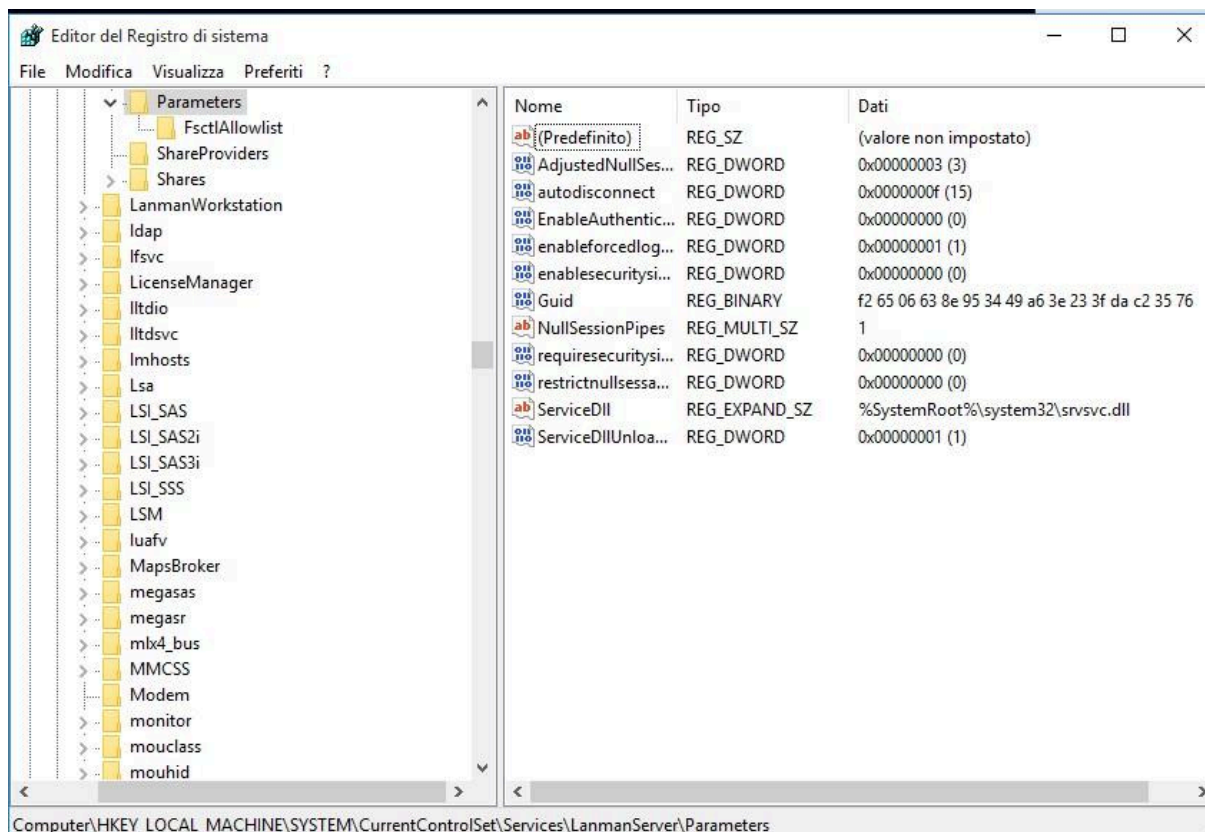


### Parte 3: Esplorazione del Registro di sistema di Windows

Il Registro di sistema di Windows è un database gerarchico che archivia la maggior parte delle impostazioni di configurazione relative al sistema operativo e all'ambiente desktop.

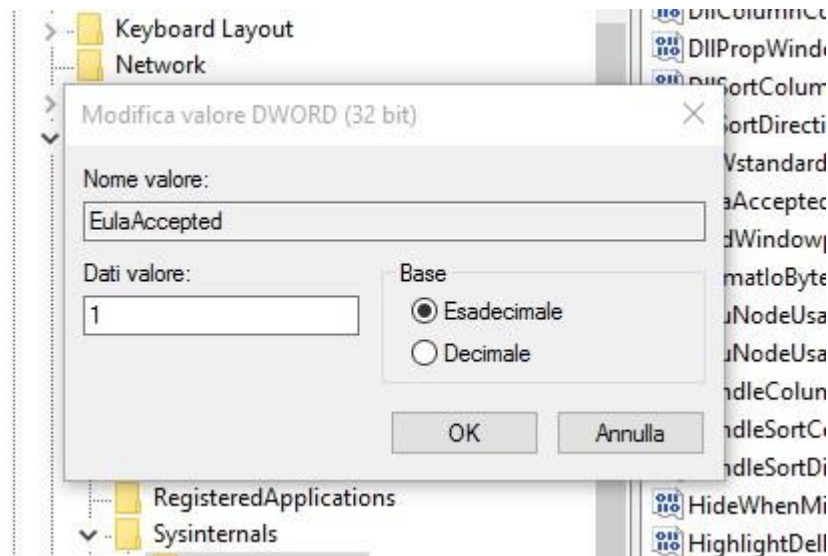
Per accedere al Registro di sistema di Windows:

1. Fai clic su **Start**.
2. Digita **regedit** nella barra di ricerca e seleziona **Editor del Registro di sistema**.



In un passaggio precedente, hai accettato l'EULA di **Process Explorer**. Ora localizzeremo la chiave di registro che registra questa azione:

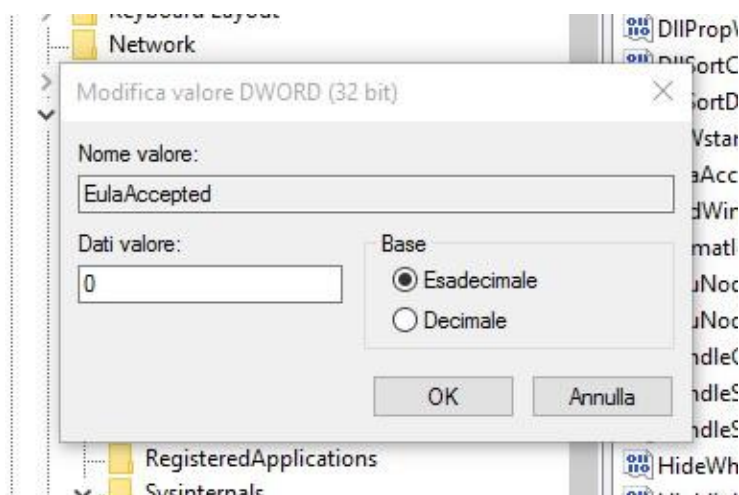
1. Vai su **HKEY\_CURRENT\_USER > Software > Sysinternals > Process Explorer**.
2. Scorri verso il basso e individua la chiave **EulaAccepted**.
  - Attualmente, il valore della chiave **EulaAccepted** è impostato su **0x00000001(1)**, il che indica che l'EULA è stato accettato dall'utente.



## Modifica della chiave di registro

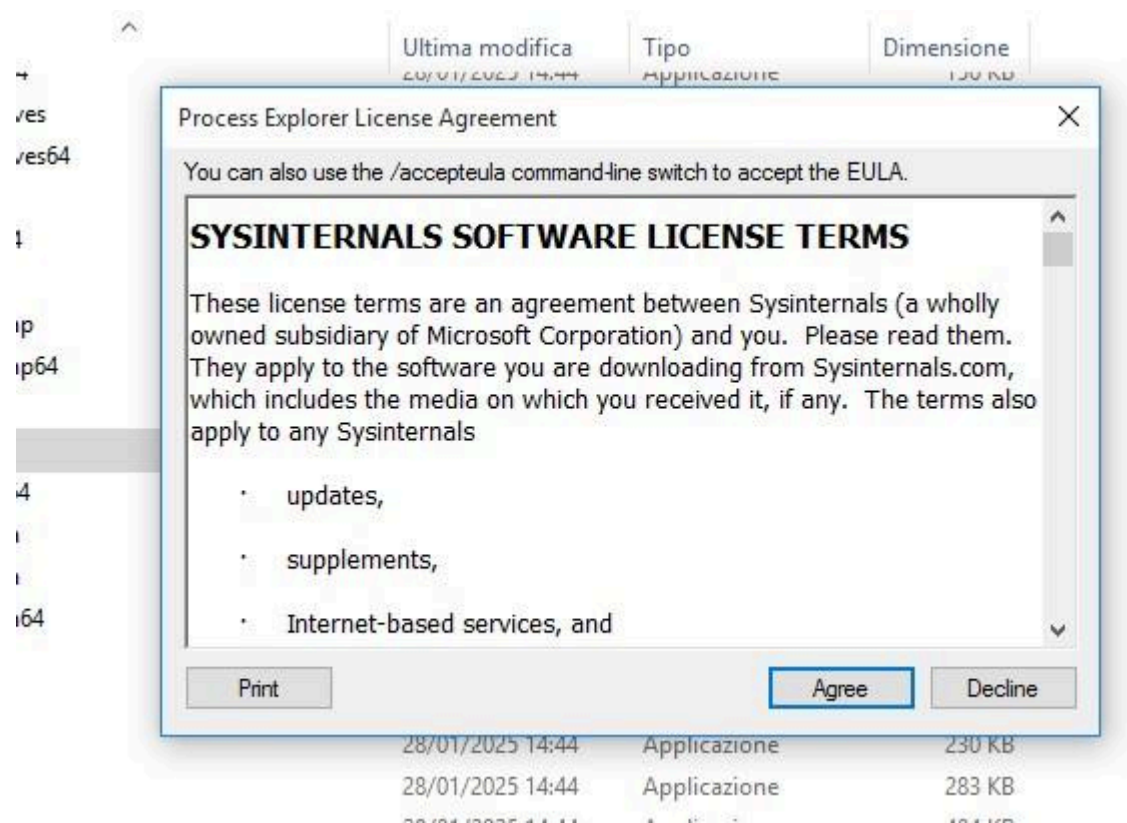
1. Fai doppio clic sulla chiave **EulaAccepted**.
2. Modifica il valore dati:
  - **Da:** 1 (EULA accettato)
  - **A:** 0 (EULA non accettato).
3. Fai clic su **OK** per salvare le modifiche.

Dopo la modifica, il valore della chiave nella colonna **Dati** è aggiornato a: **0x00000000(0)**.



## Apertura di Process Explorer

1. Vai alla cartella in cui hai scaricato il pacchetto **SysInternals**.
2. Apri la cartella **SysInternalsSuite**.
3. Fai doppio clic su **procexp.exe** per avviare **Process Explorer**.



## Risultato dell'apertura di Process Explorer

Quando hai aperto **Process Explorer**, probabilmente hai notato un'interfaccia che mostra:

- **Elenco dei processi attivi** sul sistema.
- Informazioni dettagliate su ogni processo, inclusi utilizzo della CPU, memoria e thread attivi.
- Strumenti avanzati per analizzare i processi in esecuzione e le loro dipendenze.

Questo programma è utile per il monitoraggio e il debug delle attività del sistema.