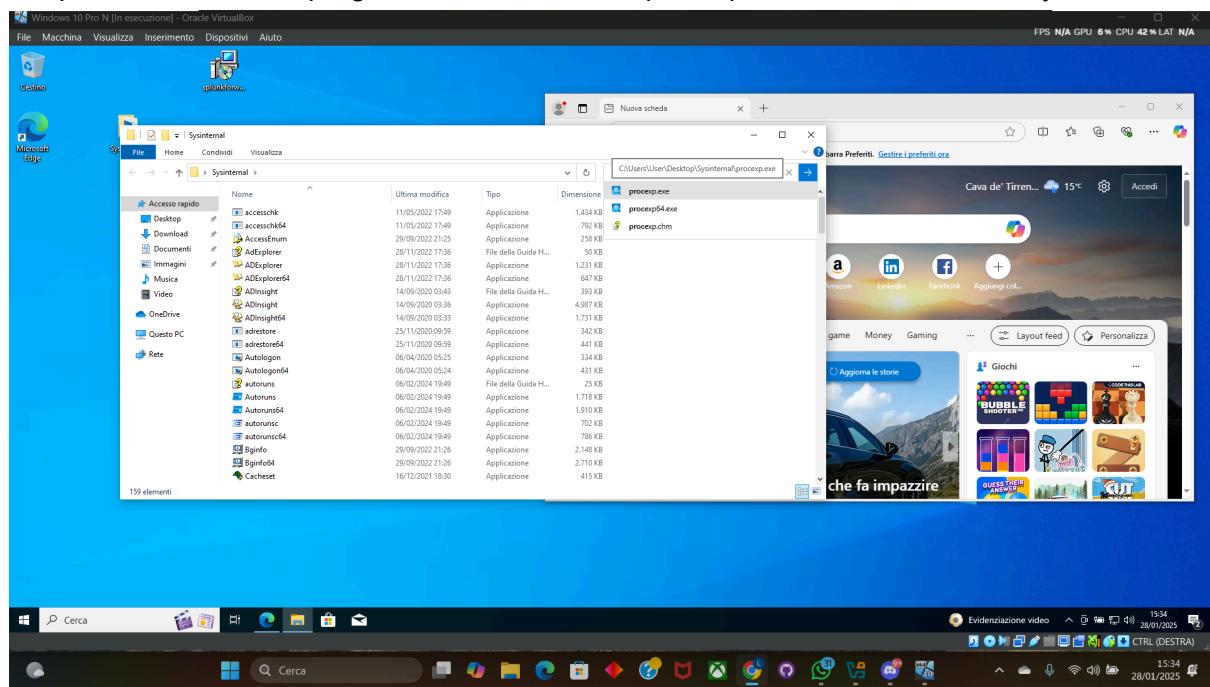


Esplorazione di Processi, Thread, Handle e Registro di Windows

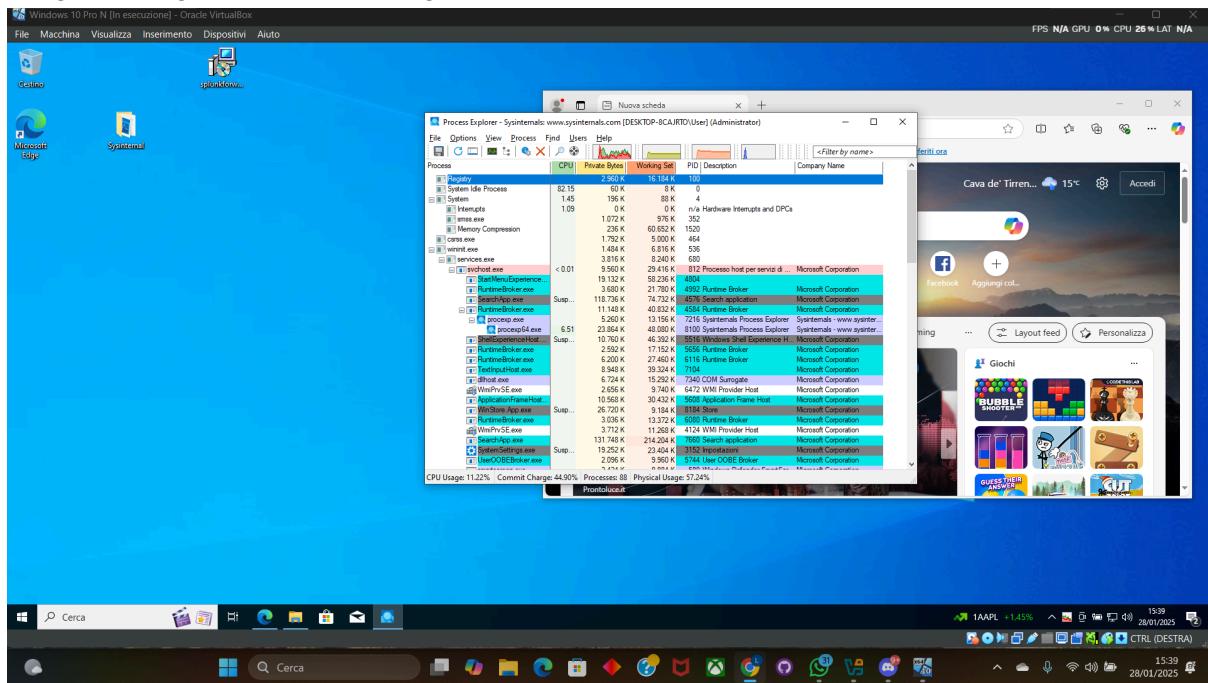
In questo laboratorio, completerai i seguenti obiettivi:

- Esplora i processi, i thread e gli handle utilizzando Process Explorer nella Sysinternals Suite.
- Utilizza il Registro di Windows per modificare un'impostazione.

Per prima cosa avvio il programma di Process Explorer presente nella suite di Sysinternals:

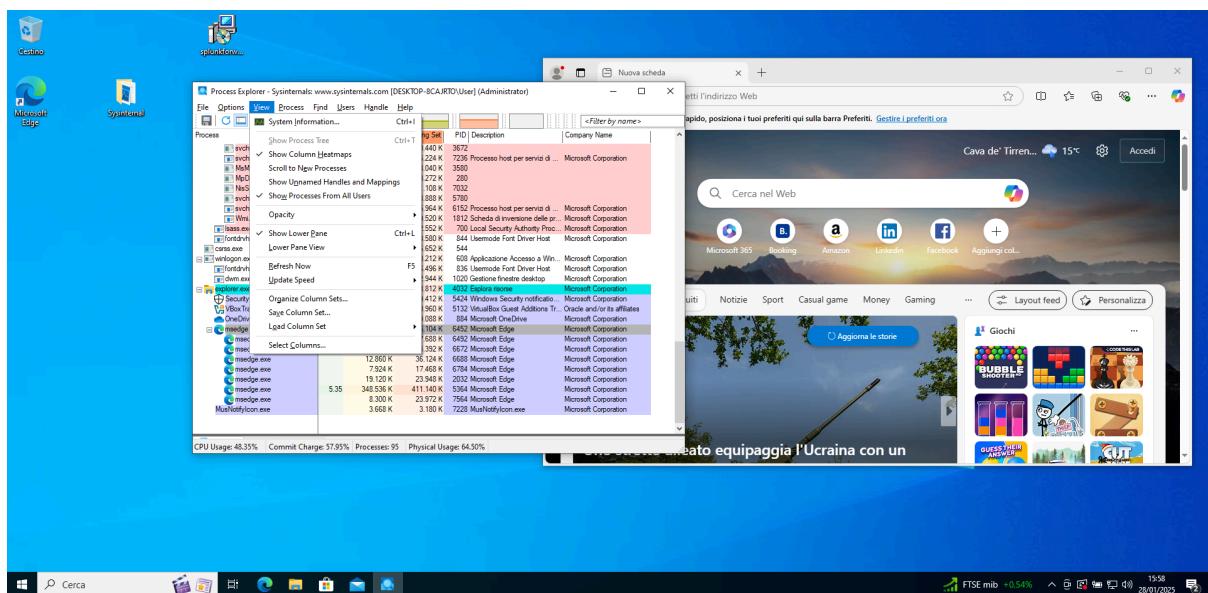


Eseguo il programma con privilegi da Amministratore:

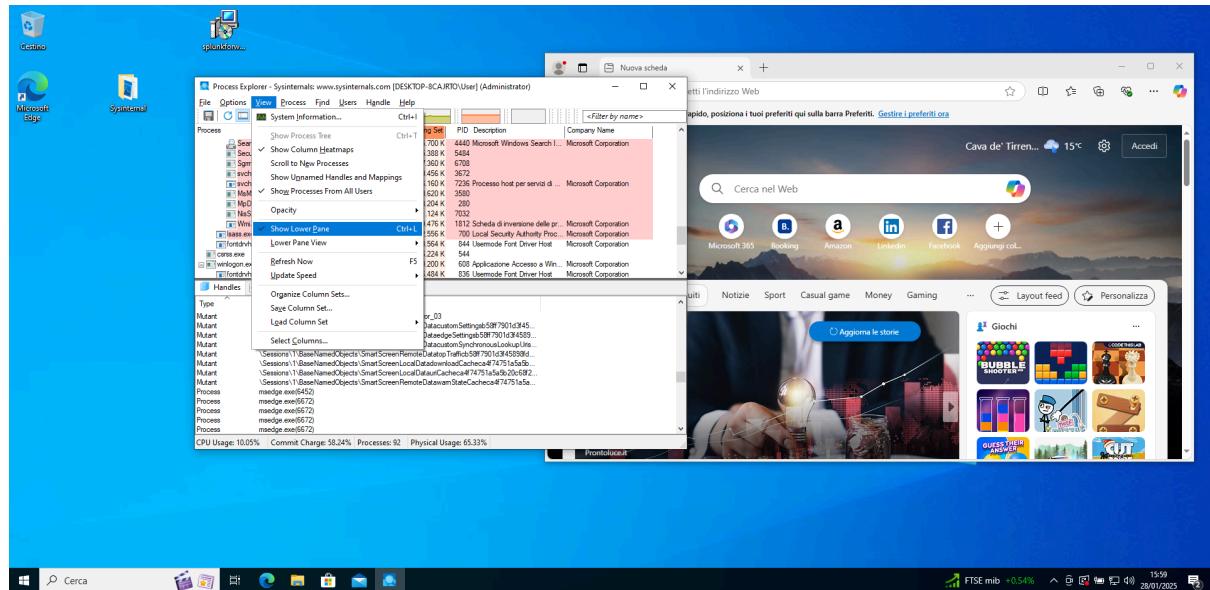


Prima di killare il processo di microsoft edge, esploriamo i vari threads e handle dei vari processi.

Per visualizzare gli handle e i threads dei vari processi su Process Explorer, bisogna recarsi nella sezione View

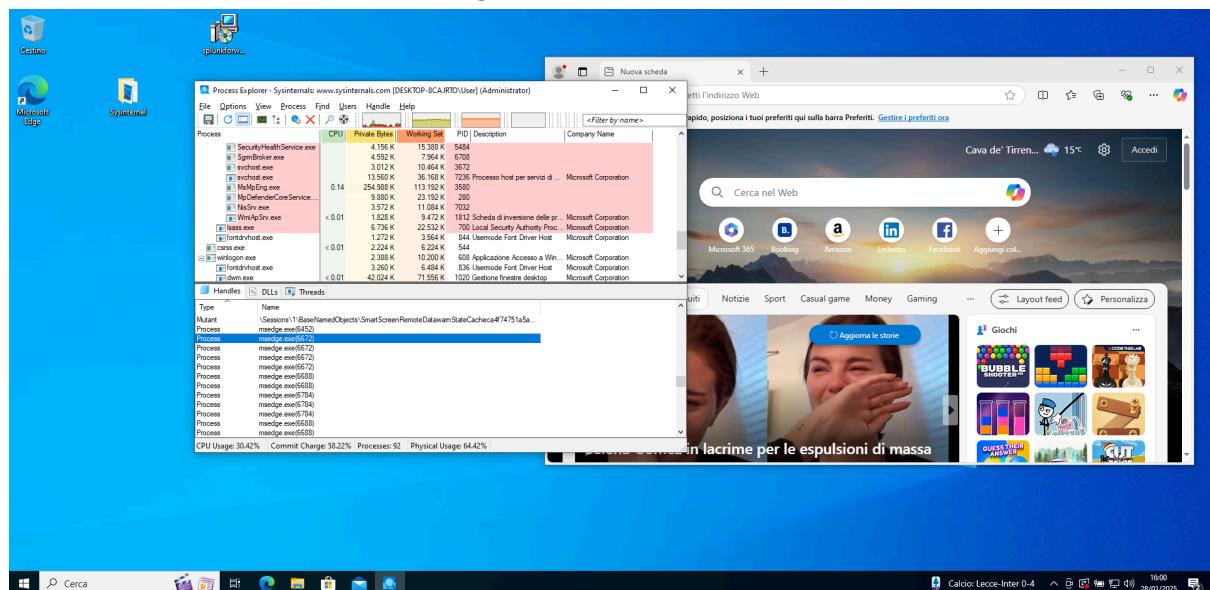


Poi selezionare la voce Show Lower Pane:

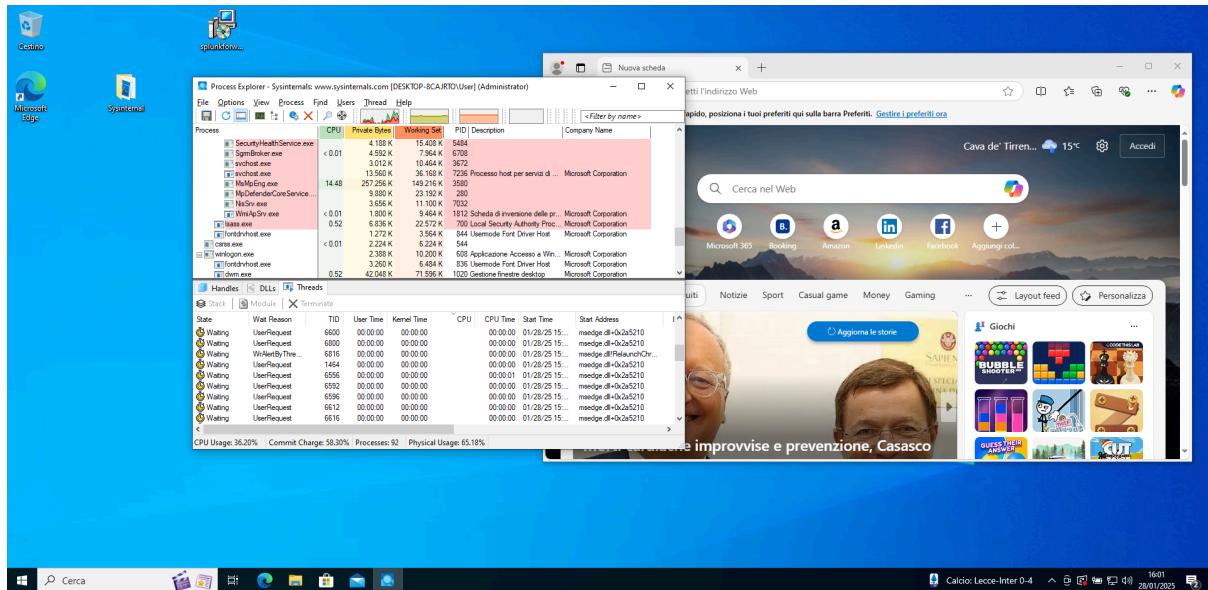


Una volta eseguiti i seguenti passaggi ci comparirà un menù dove possiamo visualizzare i vari Threads e Handle dei processi.

Handles relativi al processo di Edge:

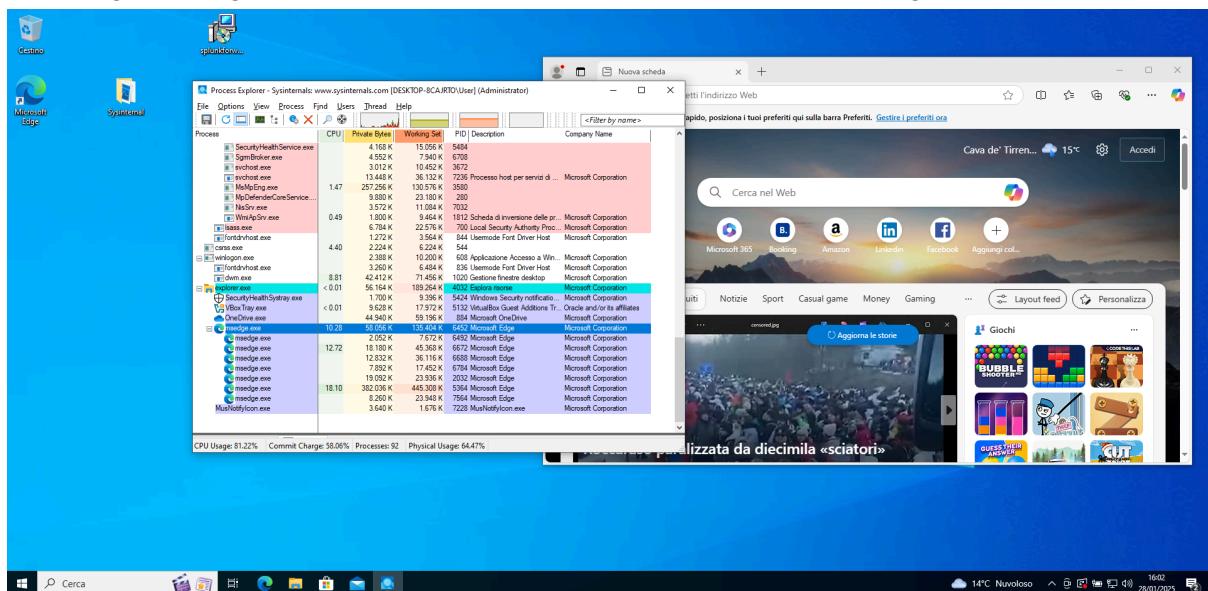


Threads relativi al processo di Edge:

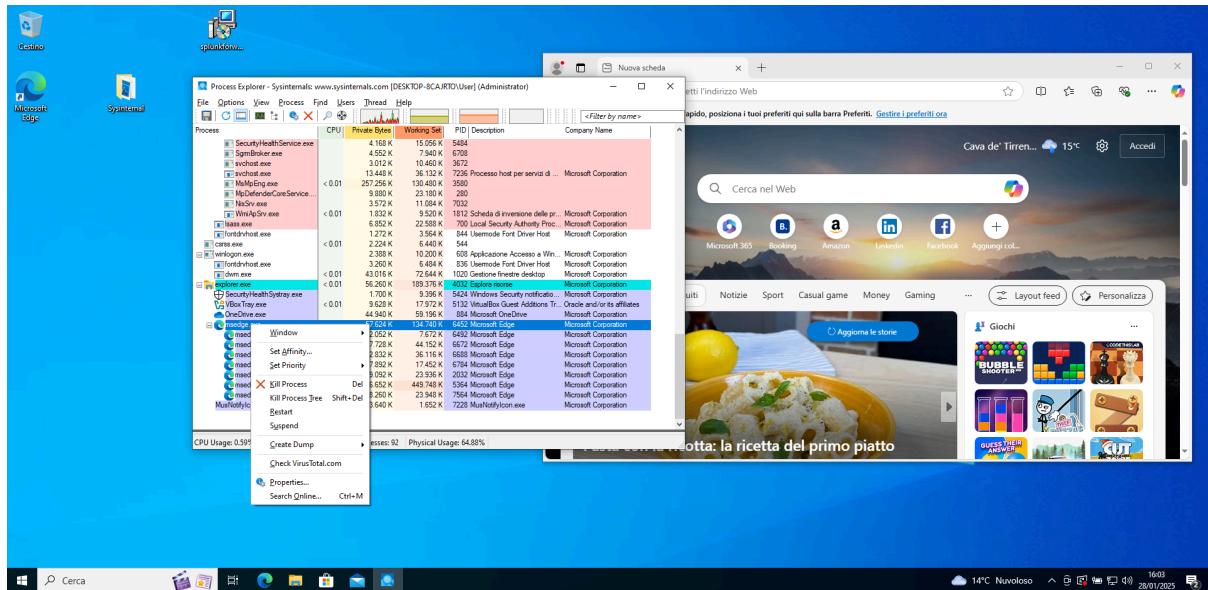


Una volta aver esplorato gli Handle e Threads possiamo proseguire killando il processo di Microsoft Edge.

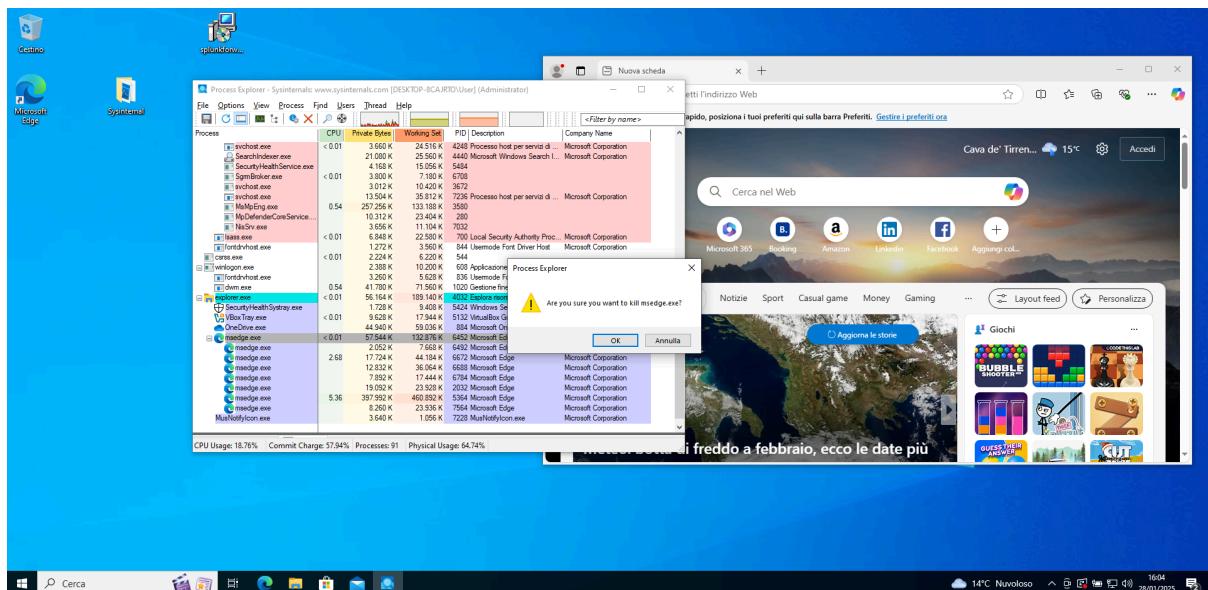
Per svolgere il seguente compito cerchiamo il processo relativo ad Edge:



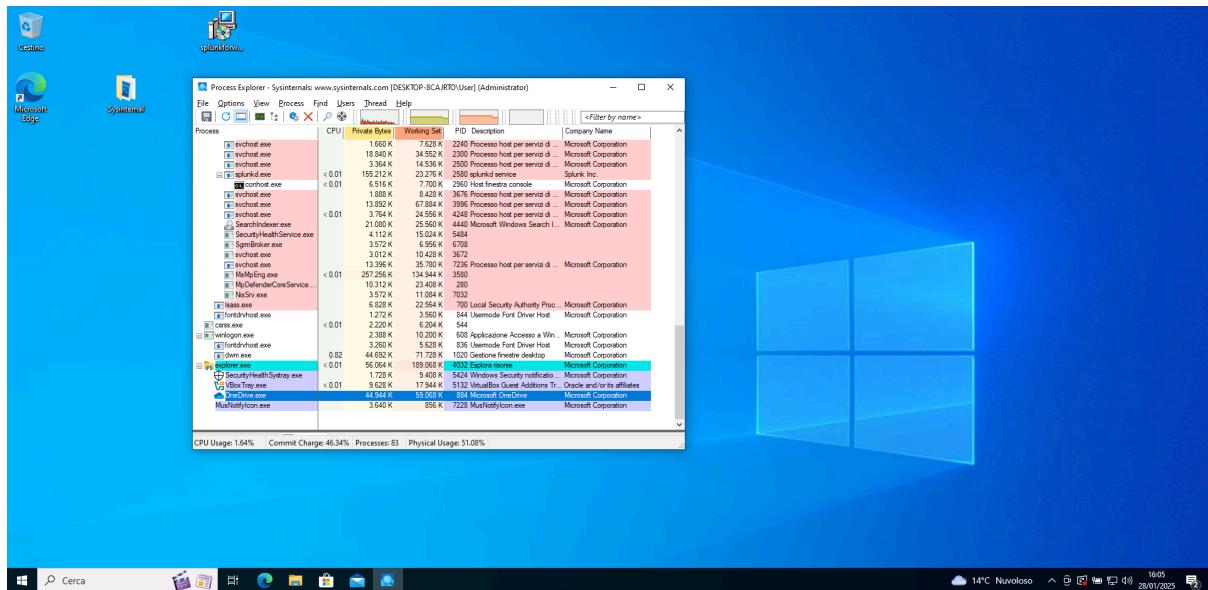
tasto destro sul processo:



E selezionare la voce “Kill Process”:



Comparirà il seguente messaggio, una volta aver cliccato ok il processo verrà killato dall'applicazione.

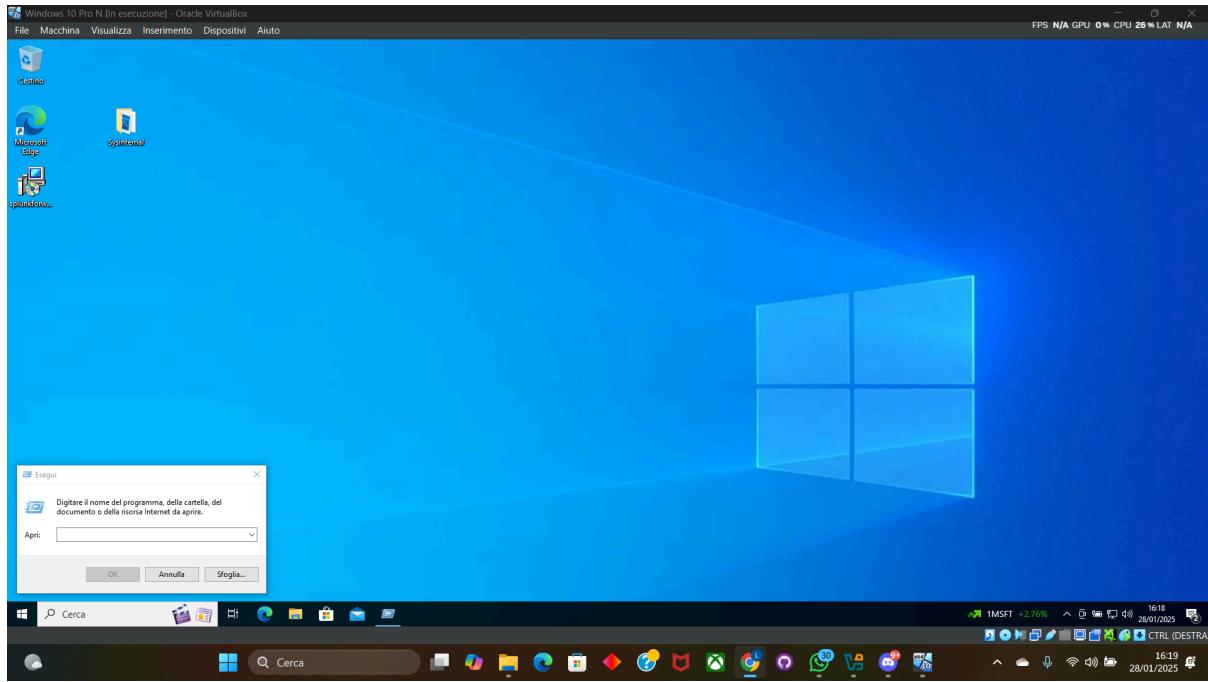


- Utilizza il Registro di Windows per modificare un'impostazione.

Per accedere al Registro di windows, recarsi in **Start** andare sulla barra di ricerca e cercare **“Eseguì”**



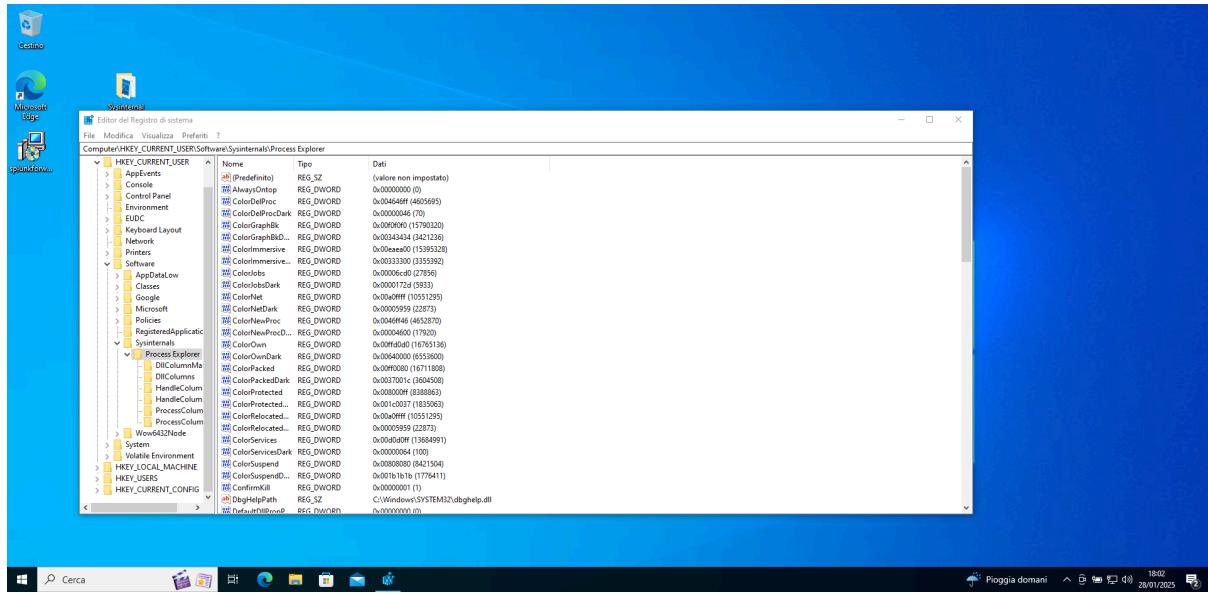
E cercare regedit



In un passaggio precedente, è stata accettata la licenza d'uso (EULA) per **Process Explorer**. Per verificare e modificare questa impostazione, ho effettuato i seguenti passaggi:

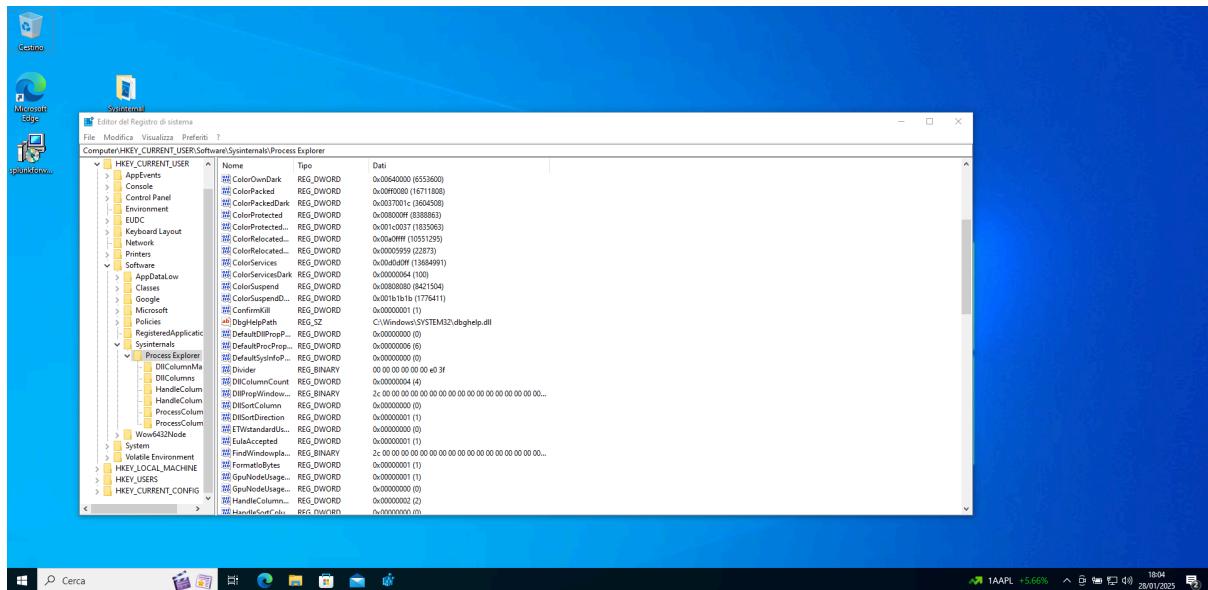
Ho aperto **Regedit** e sono andato al percorso:

HKEY_CURRENT_USER\Software\Sysinternals\Process Explorer

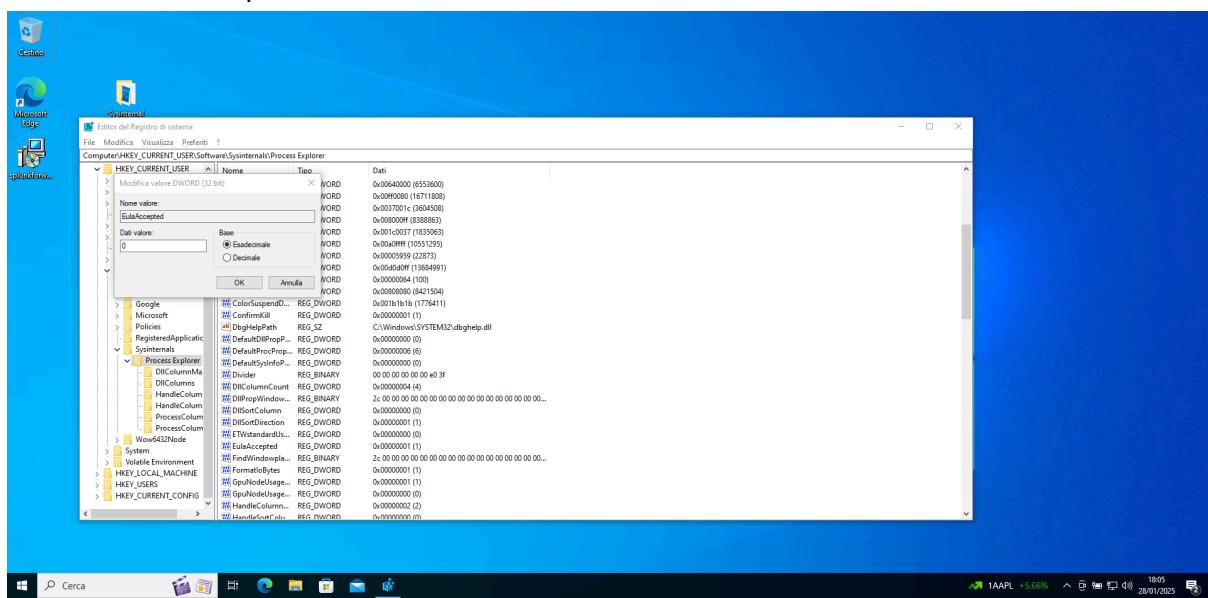


Ho selezionato la cartella **Process Explorer**.

Ho cercato la chiave **EulaAccepted** all'interno della cartella **Process Explorer**.
Il valore attuale della chiave era **0x00000001 (1)**, il che indica che l'EULA è stata accettata.



Ho fatto doppio clic sulla chiave **EulaAccepted**.
Ho cambiato il valore da **1** a **0**, indicando che l'EULA non è stata accettata.
Ho cliccato su **OK** per confermare la modifica.



- Dopo la modifica, il valore nella colonna **Dati** della chiave **EulaAccepted** è ora impostato su **0**.

Risultato Finale

La modifica ha impostato la chiave **EulaAccepted** a **0**, indicando che la licenza non è stata accettata. Questo potrebbe influenzare il comportamento di avvio di **Process Explorer**, richiedendo nuovamente l'accettazione della licenza alla prossima esecuzione.

