



S11 - L2

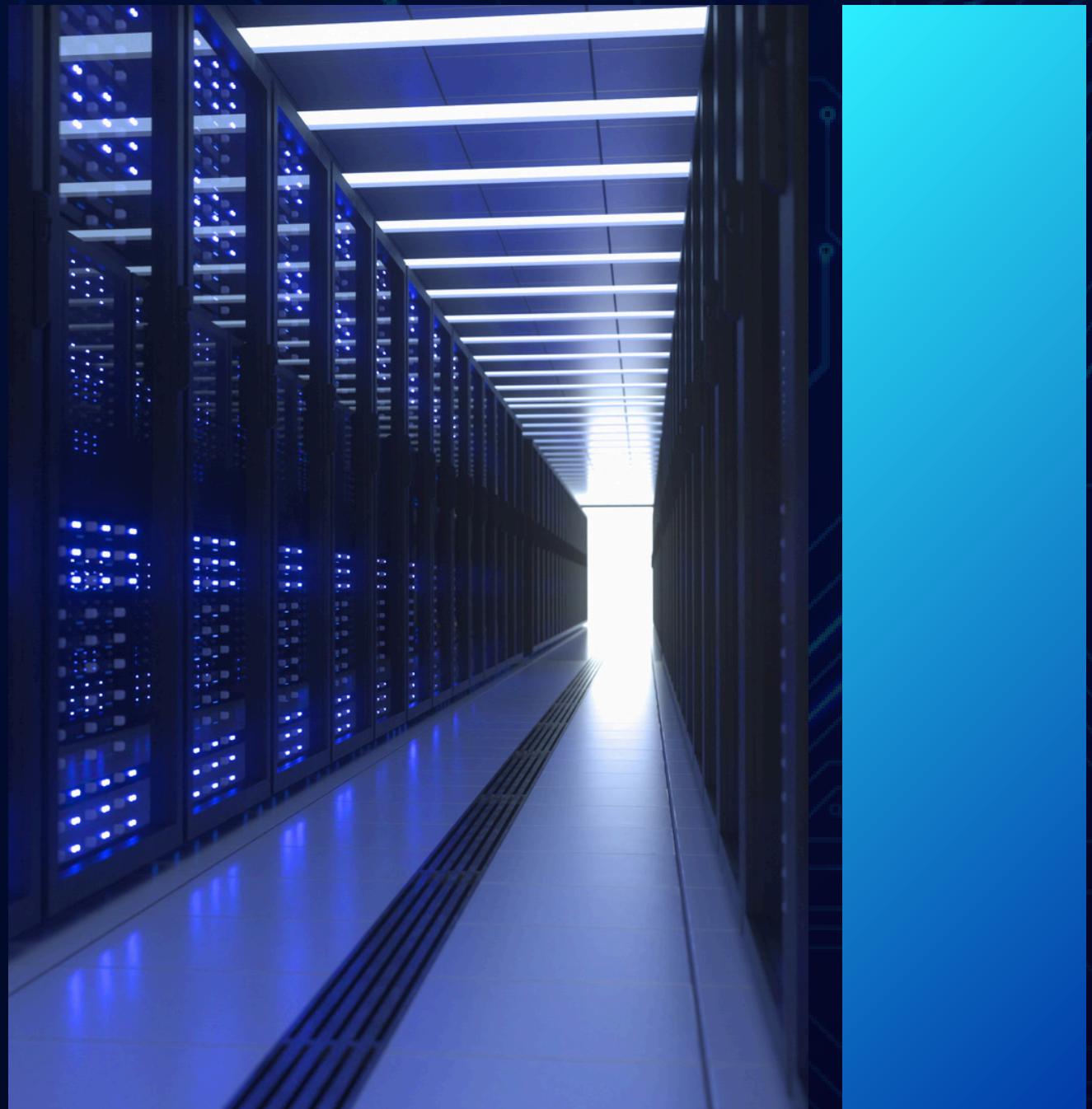
Esplorazione di Processi, Thread, Handle e Registro  
di Windows

# TRACCIA

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

In questo laboratorio, completeremo i seguenti obiettivi:

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



# ESPLORAZIONE DEI PROCESSI

Una volta scaricato Sysinternal suite e accettato i termini, ci ritroveremo davanti al process explorer. Esso è uno strumento avanzato per l'ispezione dei processi in tempo reale ed è progettato per analizzare dettagliatamente i processi, i thread, gli handle.

| Process                  | CPU     | Private Bytes | Working Set | PID   | Description                      | Company Name          |
|--------------------------|---------|---------------|-------------|-------|----------------------------------|-----------------------|
| Secure System            |         | 188 K         | 50.692 K    | 172   |                                  |                       |
| Registry                 |         | 13.528 K      | 41.464 K    | 244   |                                  |                       |
| System Idle Process      | 92.36   | 60 K          | 8 K         | 0     |                                  |                       |
| System                   | 0.09    | 48 K          | 140 K       | 4     |                                  |                       |
| Interrupts               | < 0.01  | 0 K           | 0 K         |       | n/a Hardware Interrupts and DPCs |                       |
| smss.exe                 |         | 1.152 K       | 1.068 K     | 768   |                                  |                       |
| Memory Compression       | < 0.01  | 2.568 K       | 594.620 K   | 3500  |                                  |                       |
| csrss.exe                | < 0.01  | 2.492 K       | 5.540 K     | 492   |                                  |                       |
| wininit.exe              |         | 1.564 K       | 6.060 K     | 1080  |                                  |                       |
| services.exe             | < 0.01  | 6.332 K       | 9.840 K     | 1152  |                                  |                       |
| svchost.exe              | < 0.01  | 16.656 K      | 30.968 K    | 1312  | Processo host per servizi di ... | Microsoft Corporation |
| WmiPrvSE.exe             |         | 10.328 K      | 16.176 K    | 5656  |                                  |                       |
| WmiPrvSE.exe             | < 0.01  | 15.376 K      | 27.492 K    | 6072  |                                  |                       |
| WmiPrvSE.exe             |         | 4.756 K       | 12.684 K    | 6388  |                                  |                       |
| unsecapp.exe             |         | 1.576 K       | 7.068 K     | 12020 |                                  |                       |
| SearchHost.exe           | Susp... | 253.468 K     | 98.108 K    | 1908  |                                  | Microsoft Corporation |
| StartMenuExperienceHo... | < 0.01  | 81.992 K      | 52.960 K    | 6152  | Windows Start Experience H...    | Microsoft Corporation |
| RuntimeBroker.exe        |         | 10.364 K      | 30.004 K    | 9392  | Runtime Broker                   | Microsoft Corporation |
| RuntimeBroker.exe        | < 0.01  | 20.044 K      | 44.808 K    | 5096  | Runtime Broker                   | Microsoft Corporation |
| backgroundTaskHost.exe   | Susp... | 3.928 K       | 2.092 K     | 13648 | Background Task Host             | Microsoft Corporation |
| ApplicationFrameHoste... |         | 21.612 K      | 18.060 K    | 12732 | Application Frame Host           | Microsoft Corporation |
| ShellExperienceHost.exe  | Susp... | 50.068 K      | 40.876 K    | 4672  | Windows Shell Experience H...    | Microsoft Corporation |
| RuntimeBroker.exe        |         | 6.296 K       | 19.876 K    | 13684 | Runtime Broker                   | Microsoft Corporation |
| LockApp.exe              | Susp... | 41.800 K      | 32.440 K    | 17024 | LockApp.exe                      | Microsoft Corporation |
| RuntimeBroker.exe        |         | 13.680 K      | 28.672 K    | 17464 | Runtime Broker                   | Microsoft Corporation |
| SystemSettings.exe       | Susp... | 121.696 K     | 4.252 K     | 15224 | Impostazioni                     | Microsoft Corporation |
| RtkUWP.exe               | Susp... | 35.492 K      | 7.156 K     | 1476  | Realtek Audio Console            | Realtek Semiconductor |
| RuntimeBroker.exe        |         | 2.644 K       | 11.320 K    | 1492  | Runtime Broker                   | Microsoft Corporation |
| RuntimeBroker.exe        |         | 2.232 K       | 13.616 K    | 26700 | Runtime Broker                   | Microsoft Corporation |
| Widgets.exe              |         | 8.376 K       | 35.548 K    | 68268 |                                  | Microsoft Corporation |

# ESPLORAZIONE THREAD

Prendiamo ad esempio il processo `conhost.exe` ed analizziamolo.

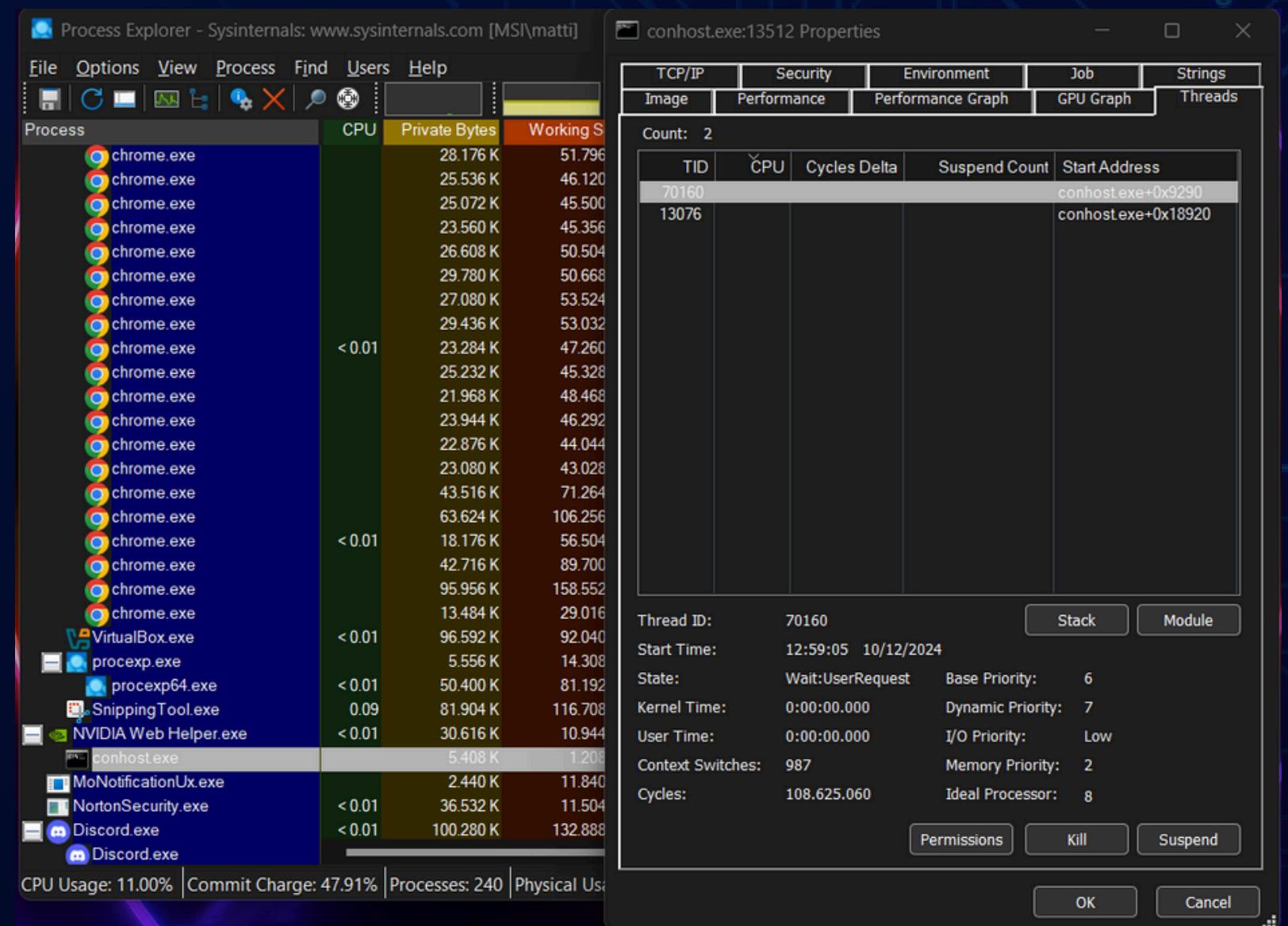
Il processo `conhost.exe` in questione è responsabile della gestione dell'interfaccia della console di comando (`cmd.exe`) e della comunicazione con il sistema.

Introdotto in Windows 7, serve a migliorare la compatibilità e la gestione grafica dei programmi console.

Prendiamo ora in esame i thread:

Nella finestra delle proprietà di `conhost.exe`, selezioniamo la scheda Threads.  
cosa si può trovare:

- ID del thread.
- Utilizzo della CPU per ciascun thread.
- Indirizzi delle funzioni chiamate (con eventuali riferimenti a DLL).

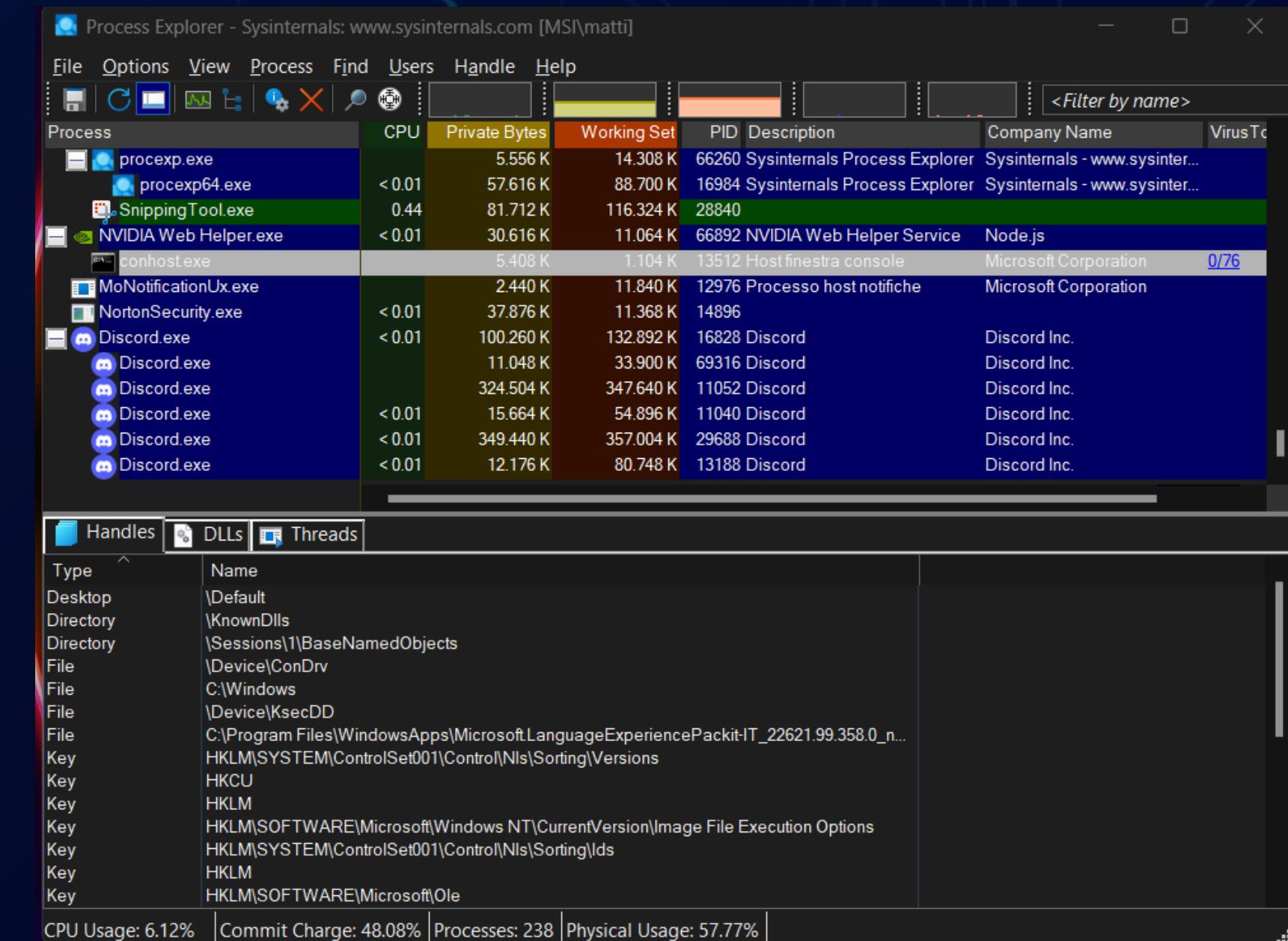


# ANALISI DEGLI HANDLE

Prendendo sempre in esame il processo `conhost.exe`, entriamo nella scheda Handles e all'interno possiamo osservare un elenco di handle aperti nel processo come ad esempio:

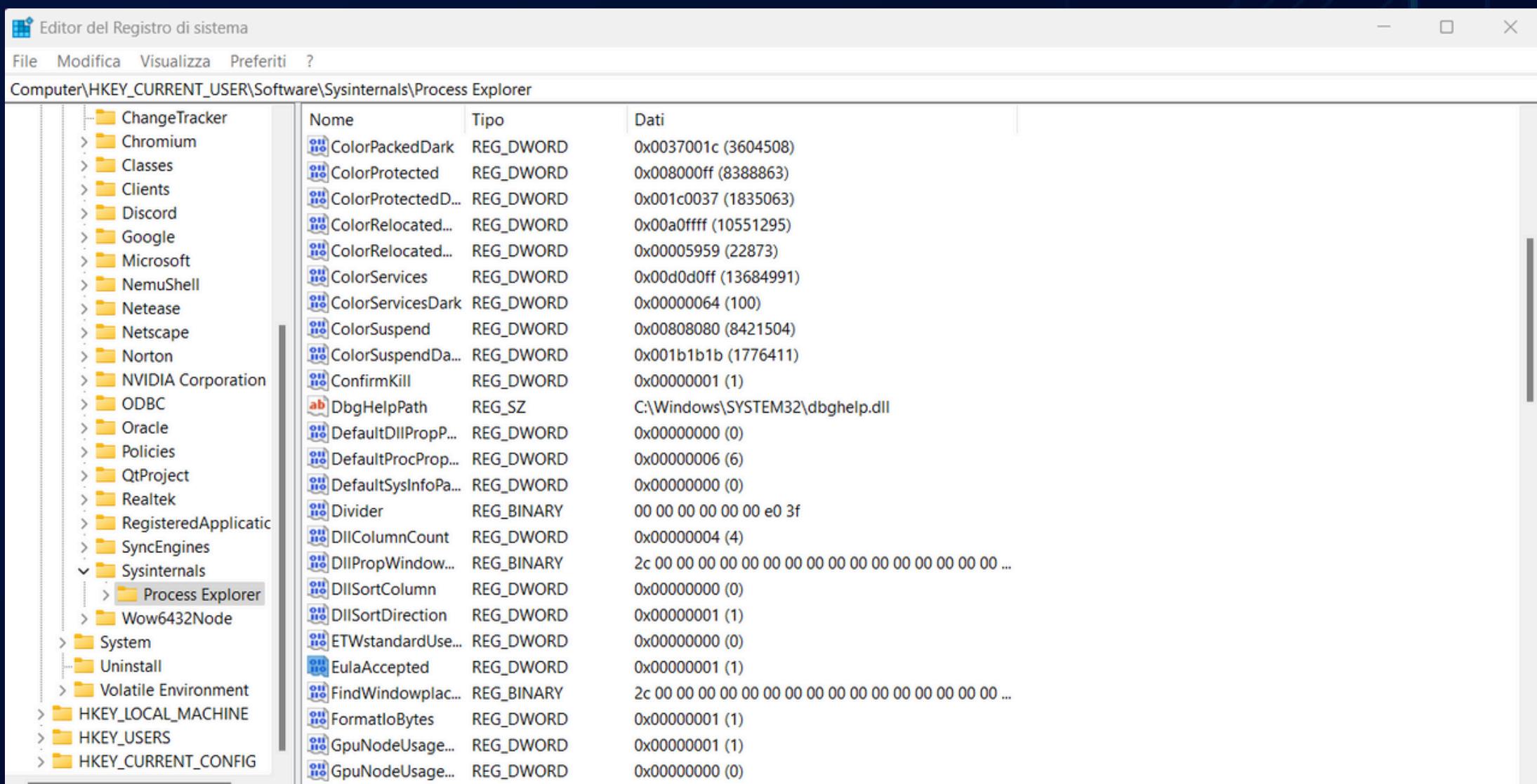
- File o cartelle aperte.
- Chiavi di registro in uso.
- Altri tipi di handle (es. pipe, eventi, mutex).

Gli handle vengono utilizzati dai processi per accedere e manipolare risorse di sistema gestite dal sistema operativo senza interagire direttamente con le loro implementazioni interne.

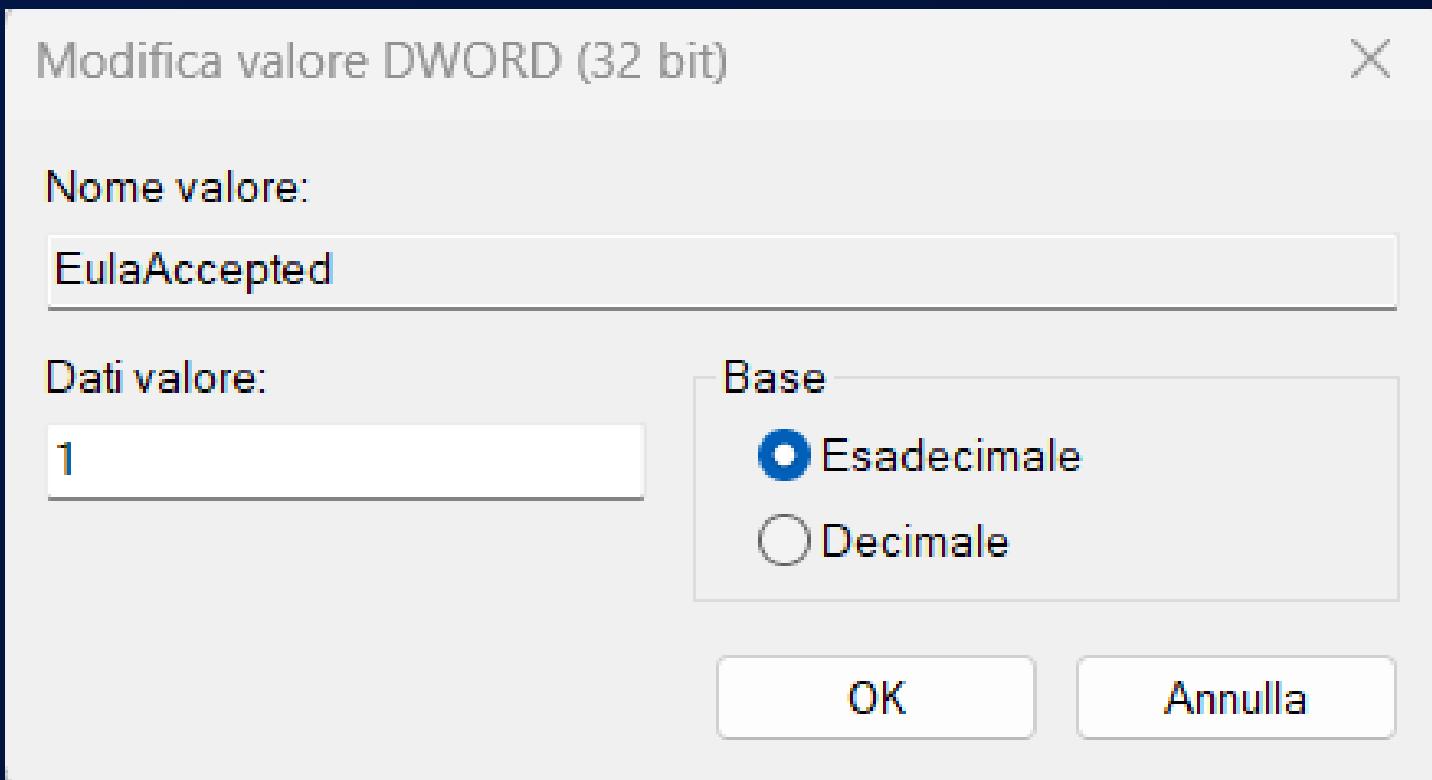


# REGISTRO DI SISTEMA

Avviamo ora il nostro registro di sistema. Entriamo nella cartella HKEY\_CURRENT\_USER > Software > SysInternals > Process Explorer. All'interno della cartella troveremo un file chiamato EulaAccepted



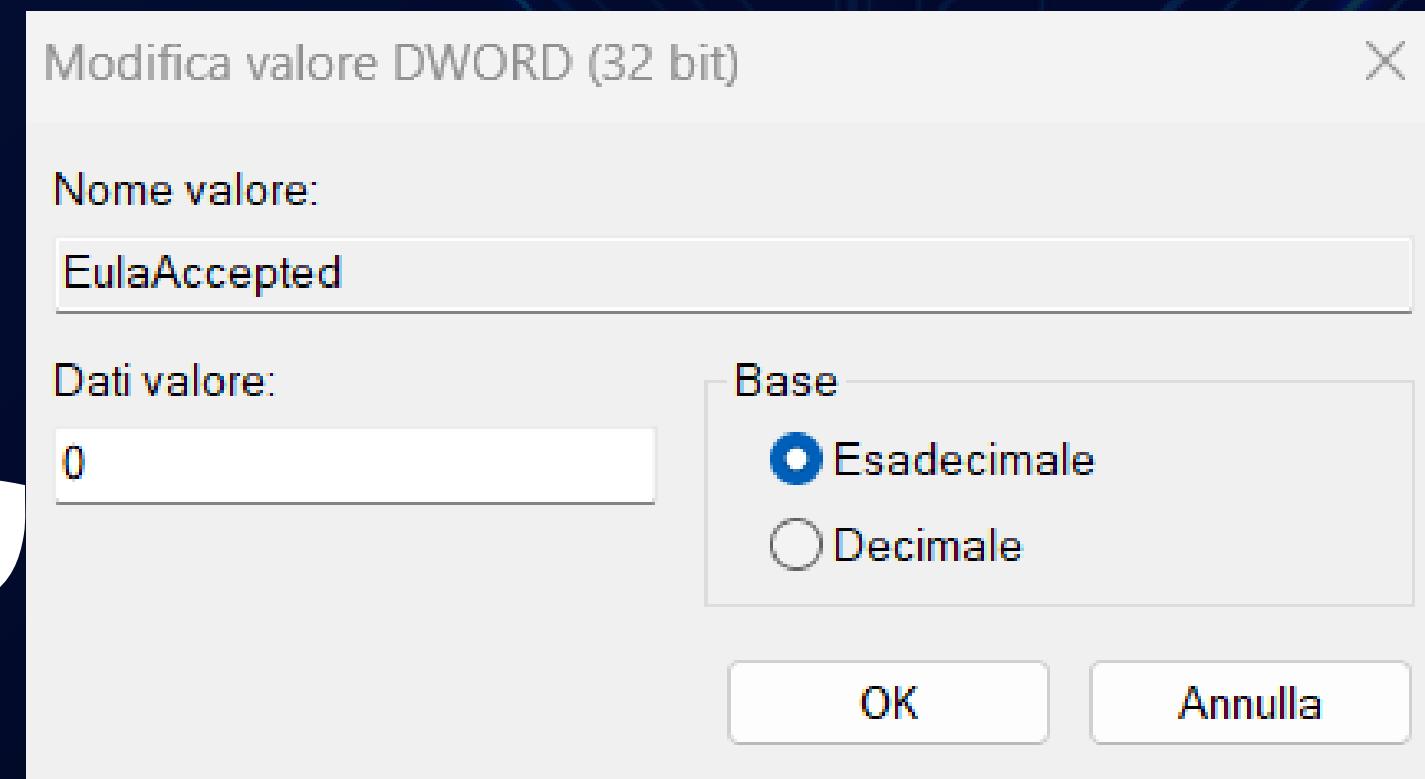
# MODIFICA IMPOSTAZIONE NEL REGISTRO DI SISTEMA



Impostiamolo ora a  
valore 0

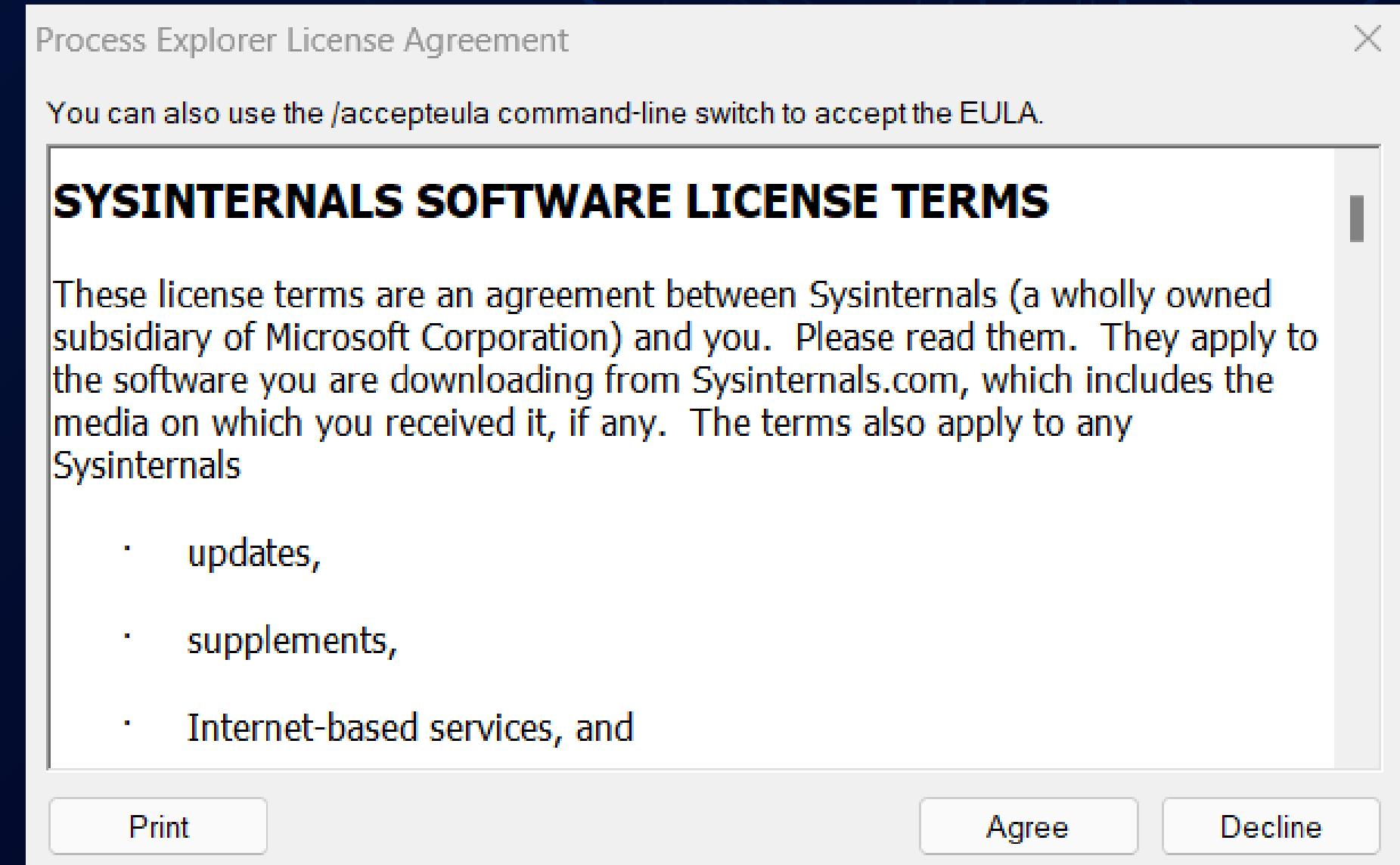


Troveremo di default il valore 1. Il valore EULA Accepted impostato a 1 nel registro di sistema di Windows indica che l'utente ha accettato i termini del contratto di licenza per l'utente finale (End User License Agreement, EULA) per un determinato software o servizio. Avendo accettato in precedenza i suddetti termini troveremo valore 1.



# MODIFICA IMPOSTAZIONE NEL REGISTRO DI SISTEMA

Impostandolo a valore 0, una volta entrati nuovamente nell'applicazione, dovremo nuovamente accettare i termini di licenza per poter accedere all'applicazione.



THANKS FOR YOUR ATTENTION

Mattia Di Donato