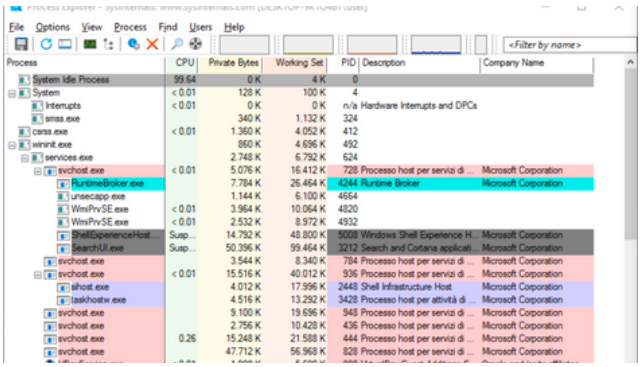
Esplorazione di Processi, Thread, Handle e Registro di Windows

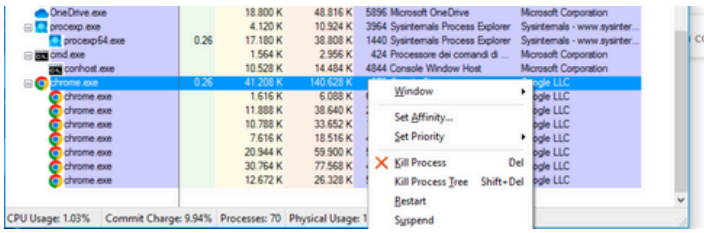
Indice

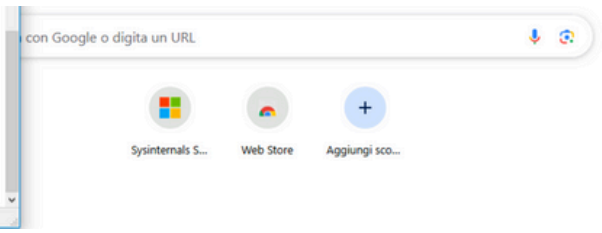
1.Esplorazione dei processi



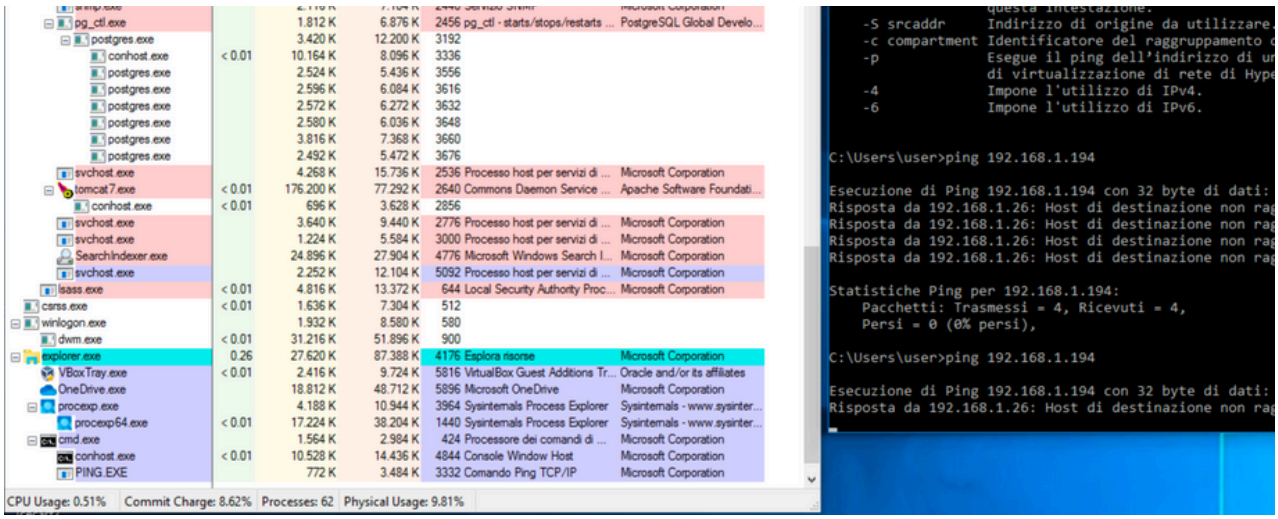
In questa parte ho esplorato i processi che sono programmi o applicazioni in esecuzione, utilizzando Process Explorer nella Windows SysInternals Suite. Inoltre, come ulteriore test, ho avviato un nuovo processo.

Trascinando l'icona del "Trova", e cliccando con il tasto destro, con kill Process, possiamo appunto chiudere il processo.



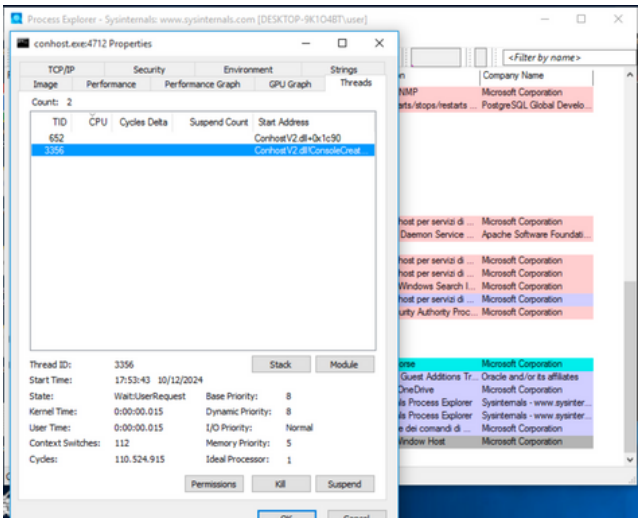


Poi ho avviato un altro processo aprendo il prompot dei comandi, che sarebbe cmd.exe. Il suo processo padre è explorer.exe. Il cmd.exe ha un processo figlio, conhost.exe.
Poi ho avviato vvia un ping al prompt per osservare i cambiamenti nel processo cmd.exe.

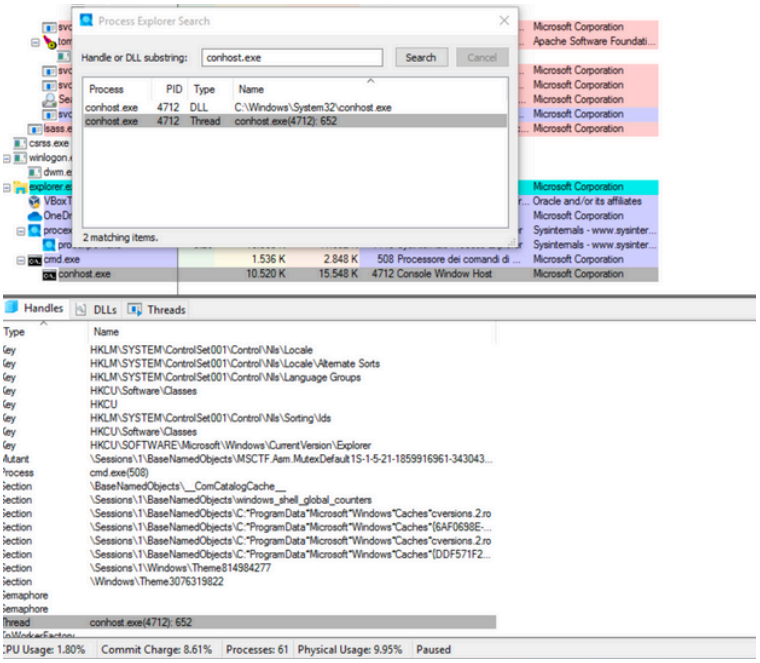


2.Esplorazione di thread e handle

In questa sezione, sono andato ad esplorare thread e handle. I processi hanno uno o più thread. Un thread è un'unità di esecuzione in un processo. Un handle è un riferimento astratto a blocchi di memoria o oggetti gestiti da un sistema operativo. Ho utilizzato Process Explorer (procexp.exe) in Windows SysInternals Suite per esplorare thread e handle.



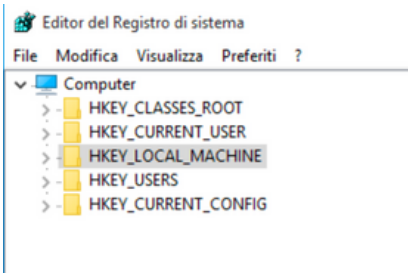
Nella finestra Process Explorer, facendoo clic con il pulsante destro del mouse su conhost.exe e selezionando Proprietà, troviamo la voce Thread, con la quale si possono visualizzare i thread attivi per il processo conhost.exe. Fai clic su OK per continuare se richiesto da una finestra di dialogo di avviso.



Poi abbiamo visualizzato l'handle facendo clic su Visualizza > selezionare Visualizzazione riquadro inferiore > Handle per visualizzare gli handle associati al processo conhost.exe. Esaminando le maniglie possiamo notare come puntano a file, chiavi di registro e thread.

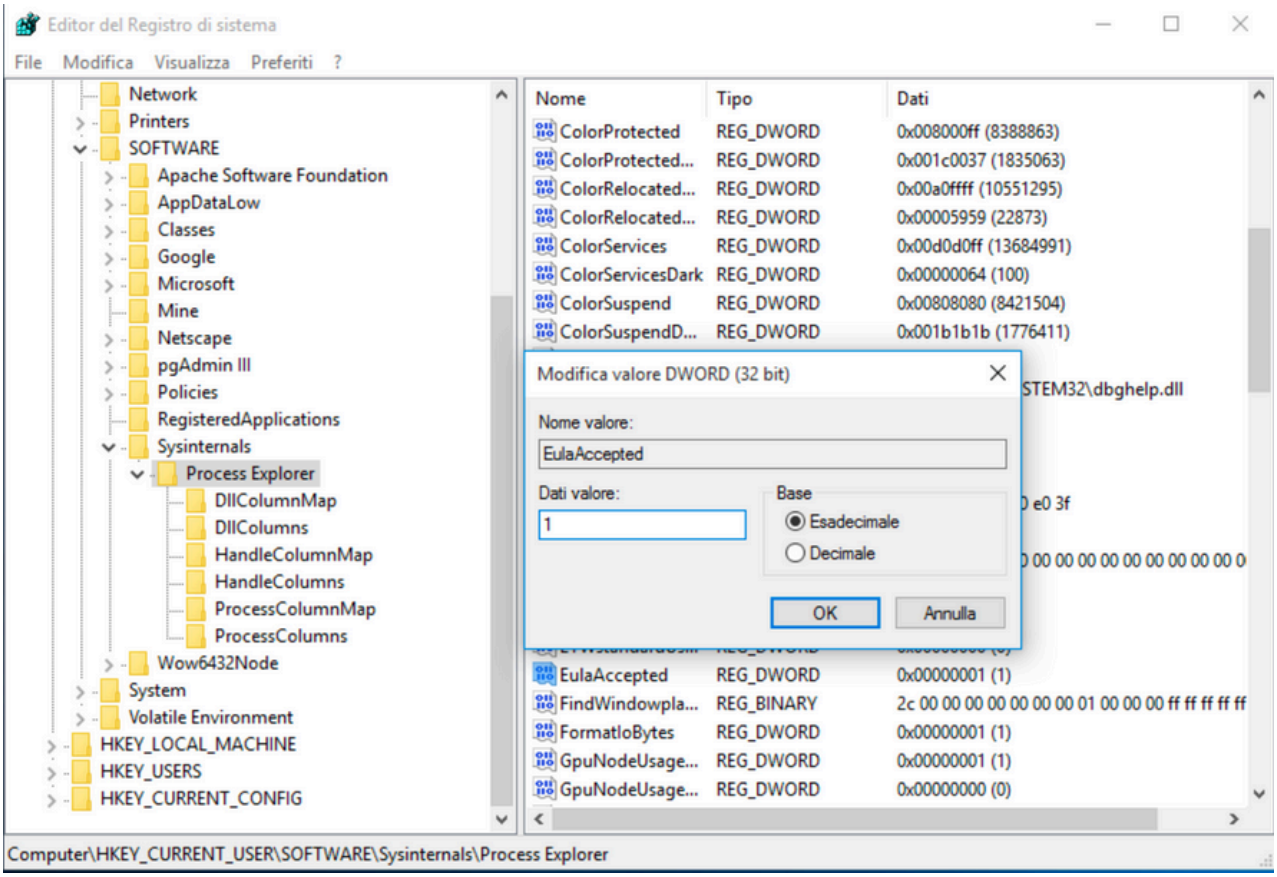
3.Esplorazione del registro di Windows

Il Registro di sistema di Windows è un database gerarchico in cui sono archiviate la maggior parte delle impostazioni di configurazione dei sistemi operativi e dell'ambiente desktop.
Per accedere al Registro di sistema di Windows, ho cercato regedit e selezionato Editor del Registro di sistema.



Il Registro di sistema di Windows è un database gerarchico in cui sono archiviate la maggior parte delle impostazioni di configurazione dei sistemi operativi e dell'ambiente desktop.
Per accedere al Registro di sistema di Windows, ho cercato regedit e selezionato Editor del Registro di sistema.

L'Editor del Registro di sistema ha cinque hive. Questi hive sono al livello superiore del registro.
HKEY_CLASSES_ROOT è in realtà la sottochiave Classes di HKEY_LOCAL_MACHINE\Software\. Memorizza informazioni utilizzate dalle applicazioni registrate come l'associazione di estensioni di file, nonché dati di un identificatore programmatico (ProgID), ID di classe (CLSID) e ID di interfaccia (IID).
HKEY_CURRENT_USER contiene le impostazioni e le configurazioni degli utenti attualmente connessi.
HKEY_LOCAL_MACHINE memorizza le informazioni di configurazione specifiche del computer locale.
HKEY_USERS contiene le impostazioni e le configurazioni per tutti gli utenti sul computer locale. HKEY_CURRENT_USER è una sottochiave di HKEY_USERS.
HKEY_CURRENT_CONFIG memorizza le informazioni hardware utilizzate all'avvio del computer locale.



Precedentemente ho accettato l'EULA per Process Explorer, perciò sono andato alla chiave di registro EulaAccepted per Process Explorer.
per selezionare Process Explorer in HKEY_CURRENT_USER > Software > Sysinternals > Process Explorer. Un volta individuata la chiave EulaAccepted, ho visto che il valore per la chiave è 0x00000001(1). Quell'1 sta ad indicare che l'EULA è stato accettato dall'utente.
Andando a modificare quel numero con lo "0" ho constatato che mi ha richiesto di accettare il contratto di licenza di Process Explorer.