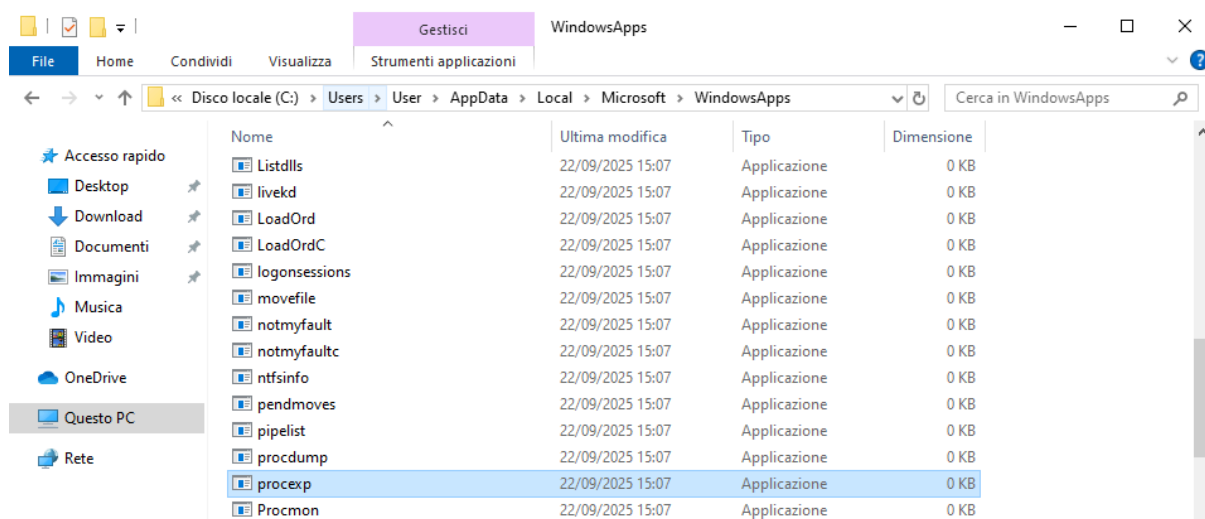


# Esplorazione di Processi, Thread, Handle e Registro di Windows

## 1. Esplorare un processo attivo

Una volta scaricato SysInternalSuite, lo eseguo andando nella sua cartella e cercando **procexp.exe**

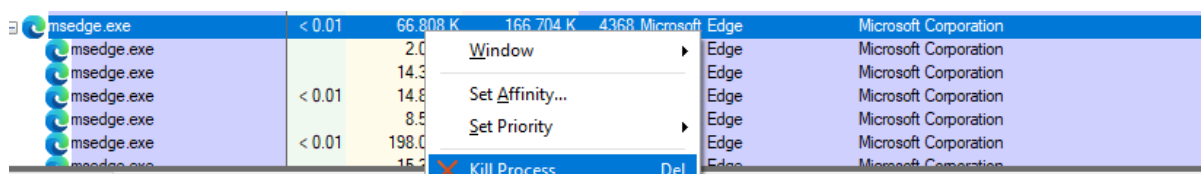


Una volta eseguito ci chiederà di accettare l'EULA e si avvierà il programma mostrandoci subito i processi attualmente attivi sul computer.

Utilizzando il pulsante Find Window's Process possiamo localizzare un processo, in questo caso cerchiamo quello del browser web. Per fare ciò trasciniamo l'icona del pulsante appunto sul browser.

regedit.exe		5.040 K	16.212 K	4616	Editor del Registro di sistema	Microsoft Corporation
procexp.exe	6.91	30.456 K	56.416 K	5248	Sysinternals Process Explorer	Sysinternals - www.sysinter...
procexp.exe	3.77	26.088 K	50.004 K	992	Sysinternals Process Explorer	Sysinternals - www.sysinter...
MusNotifylcon.exe		2.836 K	1.952 K	5928	MusNotifylcon.exe	Microsoft Corporation
msedge.exe	0.63	67.228 K	165.384 K	4368	Microsoft Edge	Microsoft Corporation
msedge.exe		2.032 K	8.196 K	4280	Microsoft Edge	Microsoft Corporation
msedge.exe	< 0.01	15.500 K	42.004 K	2260	Microsoft Edge	Microsoft Corporation
msedge.exe	7.54	15.372 K	51.996 K	5332	Microsoft Edge	Microsoft Corporation

Facendo ciò il processo viene evidenziato. Da qui lo possiamo terminare facendo tasto destro e **Kill Process**.



Il browser verrà chiuso immediatamente.

## 2. Avviare un altro processo

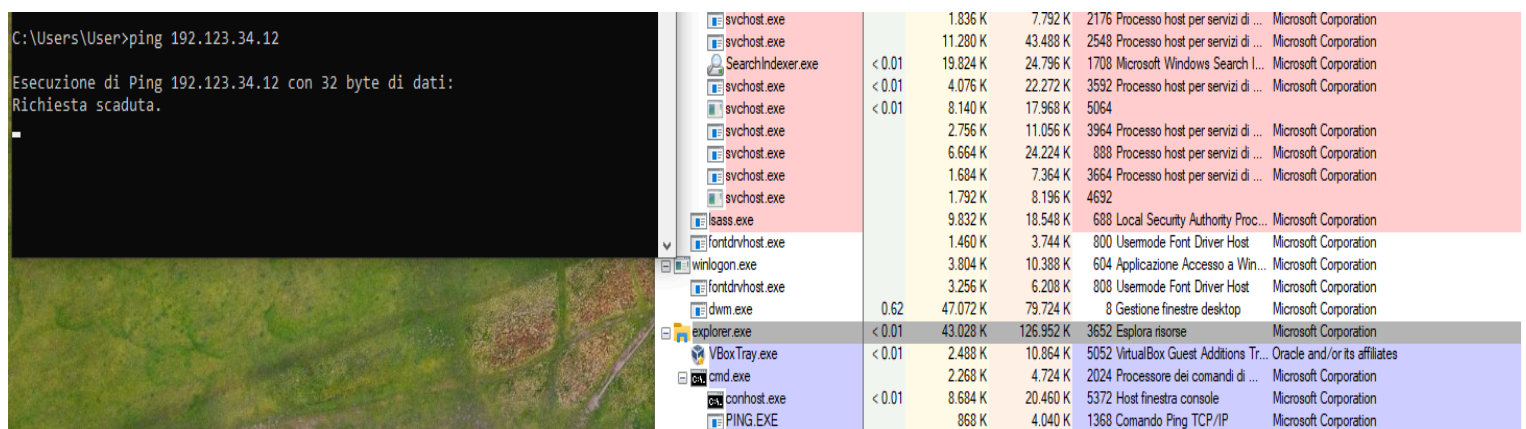
Adesso avviamo un Prompt dei comandi e, con la stessa procedura fatta per il browser, lo andiamo a localizzare all'interno del Process Explorer.



Process Name	Private Bytes	Working Set	Virtual Bytes	Process Name	Company Name
explorer.exe	42.260 K	125.936 K	3652	Esplora risorse	Microsoft Corporation
cmd.exe	2.336 K	4.740 K	2024	Processore dei comandi di ...	Microsoft Corporation
conhost.exe	8.652 K	19.284 K	5372	Host finestra console	Microsoft Corporation

Notiamo che il processo **cmd.exe** ha come processo genitore **explorer.exe** e ha come processo figlio **conhost.exe**.

Adesso avviamo un ping dal prompt dei comandi e analizziamo cosa succede su process explorer.



Command Prompt Window:

```
C:\Users\User>ping 192.123.34.12
```

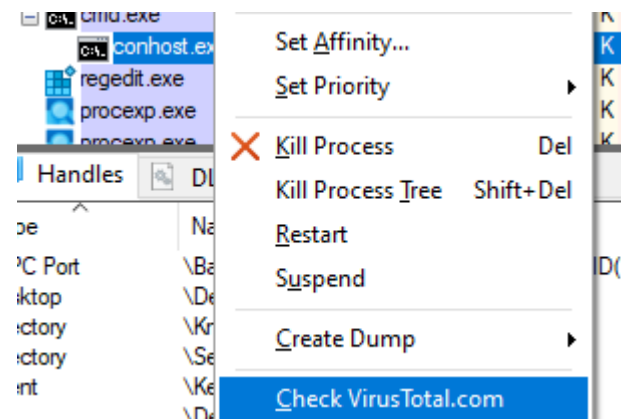
Esecuzione di Ping 192.123.34.12 con 32 byte di dati:  
Richiesta scaduta.

Process Explorer Window:

Process Name	Private Bytes	Working Set	Virtual Bytes	Process Name	Company Name
svchost.exe	1.836 K	7.792 K	2176	Processo host per servizi di ...	Microsoft Corporation
svchost.exe	11.280 K	43.488 K	2548	Processo host per servizi di ...	Microsoft Corporation
SearchIndexer.exe	< 0.01	19.824 K	24.796 K	1708 Microsoft Windows Search I...	Microsoft Corporation
svchost.exe	< 0.01	4.076 K	22.272 K	3592 Processo host per servizi di ...	Microsoft Corporation
svchost.exe	< 0.01	8.140 K	17.968 K	5064	
svchost.exe	2.756 K	11.056 K	3964	Processo host per servizi di ...	Microsoft Corporation
svchost.exe	6.664 K	24.224 K	888	Processo host per servizi di ...	Microsoft Corporation
svchost.exe	1.684 K	7.364 K	3664	Processo host per servizi di ...	Microsoft Corporation
svchost.exe	1.792 K	8.196 K	4692		
lsass.exe	9.832 K	18.548 K	688	Local Security Authority Proc...	Microsoft Corporation
fontdrvhost.exe	1.460 K	3.744 K	800	Usemode Font Driver Host	Microsoft Corporation
winlogon.exe	3.804 K	10.388 K	604	Applicazione Accesso a Win...	Microsoft Corporation
fontdrvhost.exe	3.256 K	6.208 K	808	Usemode Font Driver Host	Microsoft Corporation
explorer.exe	< 0.01	43.028 K	126.952 K	3652 Esplora risorse	Microsoft Corporation
VBoxTray.exe	< 0.01	2.488 K	10.864 K	5052 VirtualBox Guest Additions Tr...	Oracle and/or its affiliates
cmd.exe	< 0.01	2.268 K	4.724 K	2024 Processore dei comandi di ...	Microsoft Corporation
conhost.exe	< 0.01	8.684 K	20.460 K	5372 Host finestra console	Microsoft Corporation
PING.EXE	868 K	4.040 K	1368	Comando Ping TCP/IP	Microsoft Corporation

Vediamo che sotto a cmd.exe compare un nuovo processo chiamato PING.exe

Da Process Explorer, possiamo anche visualizzare se un processo è malevolo. Possiamo fare ciò cliccando con il tasto destro sul processo desiderato e cliccare Check [VirusTotal.com](https://www.virustotal.com)



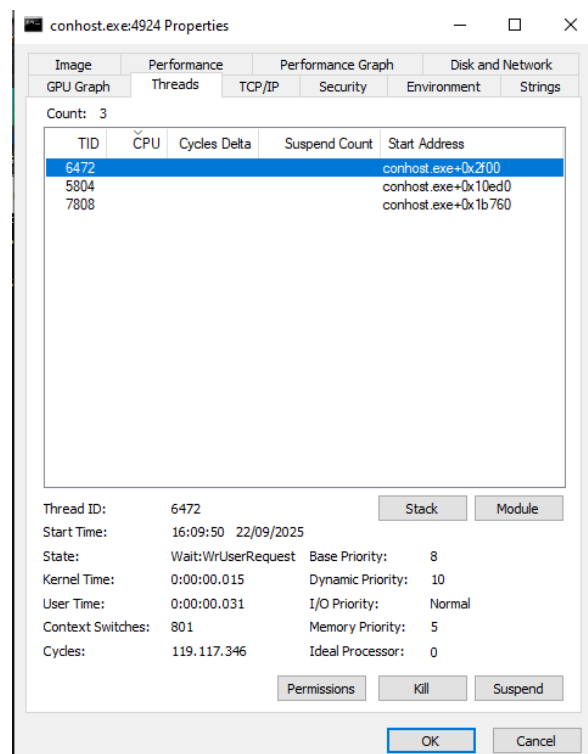
Vedremo comparire a destra un valore, quel valore è il punteggio che ha ottenuto il processo su VirusTotal, in questo caso otteniamo 0/77, il che vuol dire che il processo non è malevolo. Cliccando su quel valore si aprirà la pagina di VirusTotal



Facendo Kill Process su cmd.exe vedremo chiudersi anche il processo conhost.exe, essendo un processo figlio.

### 3. Esplorazione di Thread e Handle

Per esplorare i Thread facciamo tasto destro su un processo e clicchiamo su Proprietà.



La parte superiore della finestra elenca tutti i thread attivi per questo processo. Per ogni thread, vengono fornite le seguenti informazioni:

- **TID (Thread ID):** L'identificatore numerico univoco del thread.

- **CPU:** La percentuale di utilizzo della CPU da parte di quel singolo thread. In questo caso è vuota, indicando un utilizzo nullo o trascurabile al momento della cattura dell'immagine.
- **Cycles Delta:** Il numero di cicli di CPU utilizzati dal thread dall'ultimo aggiornamento, una misura precisa della sua attività.
- **Suspend Count:** Indica quante volte il thread è stato sospeso.
- **Start Address:** L'indirizzo di memoria da cui il thread ha iniziato la sua esecuzione. Indica la funzione che il thread è stato creato per eseguire.

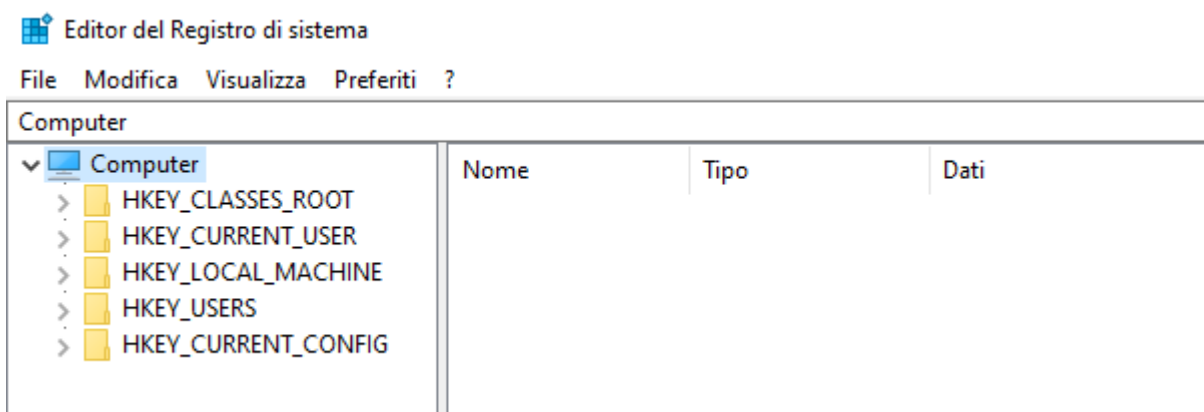
Per esplorare gli handle invece facciamo, in Process Explorer, clic su View V> selezionare Lower Pane View > Handles per visualizzare gli handle associati al processo conhost.exe. Si aprirà un pannello inferiore.

Handles		DLLs	Threads
Type	Name		
ALPC Port	\BaseNamedObjects\{Core UI}-PID(4924)-TID(6472) 9f6598d5-5819-445f-81fc-702e66676412		
Desktop	\Default		
Directory	\KnownDlls		
Directory	\Sessions\1\BaseNamedObjects		
Event	\KernelObjects\MaximumCommitCondition		
File	\Device\ConDrv		
File	C:\Windows		
File	\Device\KsecDD		
File	C:\Program Files\WindowsApps\Microsoft.LanguageExperiencePackit-IT_19041.80.274.0_...		
File	\Device\CNCG		
File	C:\Program Files\WindowsApps\Microsoft.LanguageExperiencePackit-IT_19041.80.274.0_...		
File	\Device\DeviceApi		
File	C:\Windows\Fonts\StaticCache.dat		
File	C:\Program Files\WindowsApps\Microsoft.LanguageExperiencePackit-IT_19041.80.274.0_...		
File	C:\Windows\WinSxS\amd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0_...		
Key	HKLM\SYSTEM\ControlSet001\Control\Nls\Sorting\Versions		

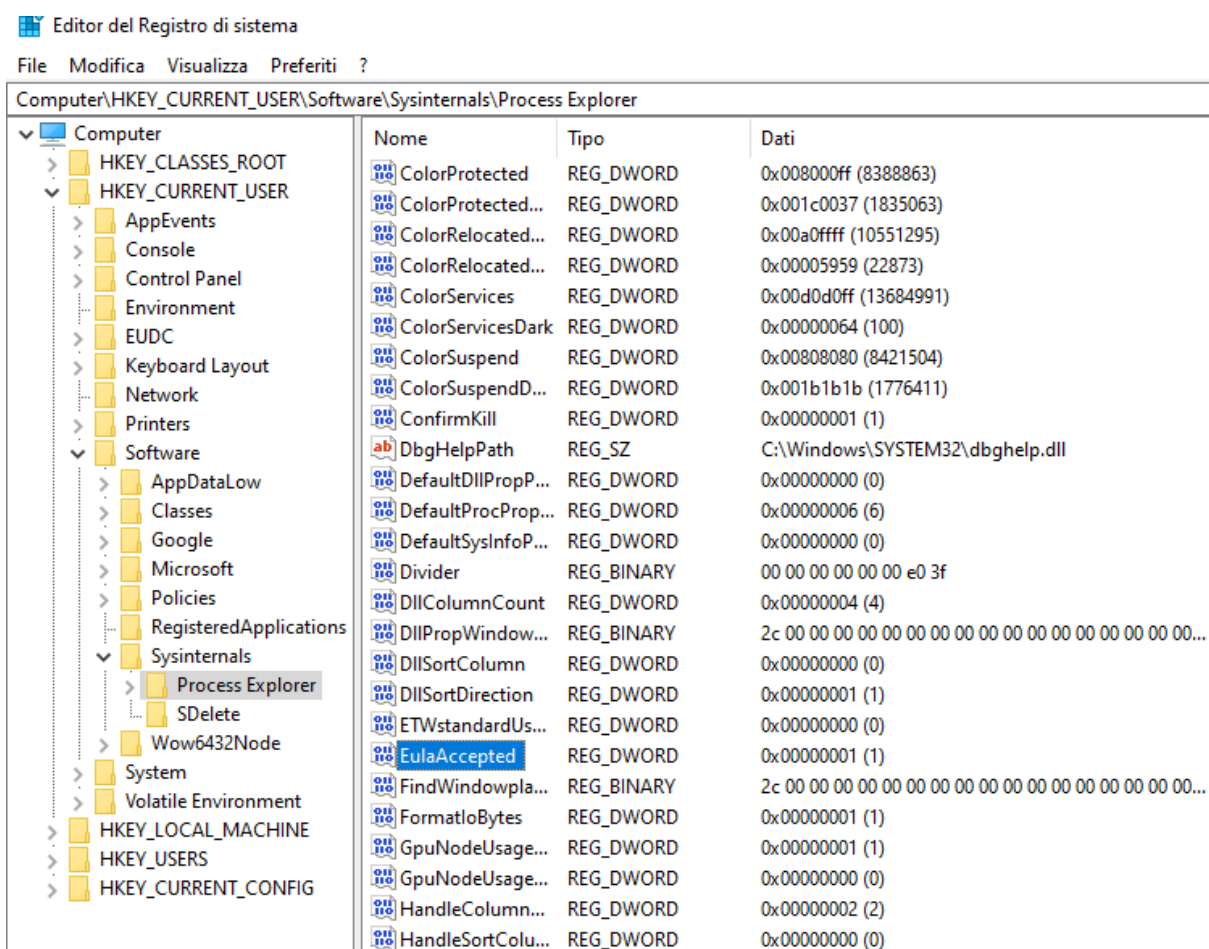
Gli handle puntano a due tipi principali di risorse di sistema: **File** e **Chiavi di registro (Key)**. Un "handle" è essenzialmente un riferimento, un puntatore che un programma utilizza per accedere a una risorsa specifica gestita dal sistema operativo. Gli handle di tipo file puntano a file fisici sul disco, ma anche a "device" (dispositivi) che vengono trattati dal sistema come se fossero file. Mentre gli handle di tipo key puntano a chiavi specifiche all'interno del **Registro di Sistema di Windows**. Il registro è un database gerarchico che contiene le impostazioni e le configurazioni per il sistema operativo e per le applicazioni installate.

#### 4. Esplorazione del Registro di Windows

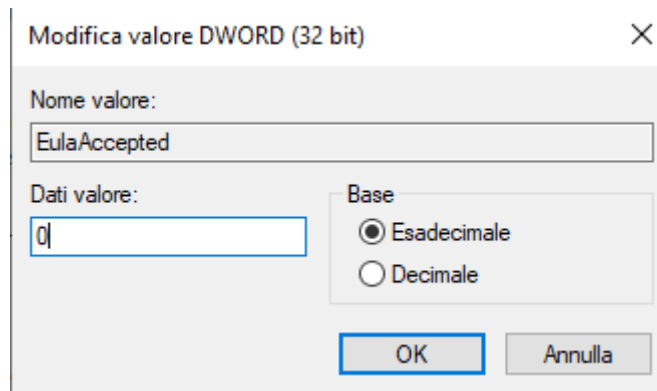
Per accedere al Registro di Windows, fare clic su Start > Cercare regedit e selezionare Editor del Registro di sistema. Si aprirà questa pagina:



Da qui andiamo a modificare la chiave di registro relativa all'EULA che abbiamo accettato una volta avviato Process Explorer. Navighiamo in HKEY\_CURRENT\_USER Software > Sysinternals > Process Explorer e cerchiamo la chiave EulaAccepted.



Notiamo che il valore è impostato a 1, il che vuol dire che è stata accettata dall'utente. Facendo doppio clic si aprirà la pagina per modificare il valore, andiamo ad inserire 0, ovvero che non è stata accettata dall'utente



Quando riavvio il process explorer mi viene richiesto di accettare l'EULA.

## Conclusione

L'esplorazione di processi, thread, handle e Registro di Windows con Sysinternals Process Explorer ha dimostrato l'importanza di questi strumenti per la comprensione e la gestione del sistema operativo. Abbiamo imparato a identificare e manipolare i processi, analizzare i thread, gestire gli handle e modificare il Registro. L'uso di Process Explorer e dell'Editor del Registro offre un controllo granulare e una visione dettagliata di Windows, fondamentali per la risoluzione dei problemi, l'ottimizzazione e l'analisi della sicurezza.