

Esplorazione di Processi, Thread, Handle e Registro di Windows

1) Esplorare un processo attivo.

Cosa è successo alla finestra del browser web quando il processo è stato terminato?

opera.exe	< 0.01	194.088 K	238.388 K	13412 Opera Internet Browser	Opera Software
opera.exe	< 0.01	23.292 K	51.832 K	4416 Opera Internet Browser	Opera Software
opera.exe		9.016 K	24.312 K	5868 Opera Internet Browser	Opera Software
opera.exe		29.816 K	67.532 K	5884 Opera Internet Browser	Opera Software
opera.exe		14.856 K	35.492 K	13232 Opera Internet Browser	Opera Software

La finestra del browser si è chiusa dopo aver effettuato **Kill Process**.

2) Navigare alla finestra del Prompt dei Comandi. Avviare un ping al prompt.

Cosa è successo durante il processo ping?

cmd.exe	< 0.01	3.064 K	5.752 K	5456 Processore dei comandi di ...	Microsoft Corporation
conhost.exe		1.408 K	9.592 K	4484 Host finestra console	Microsoft Corporation
PING.EXE	< 0.01	1.080 K	6.188 K	2628 Comando Ping TCP/IP	Microsoft Corporation

Durante l'utilizzo del comando **ping** sul cmd, si è aperto un nuovo processo chiamato **PING.EXE** sotto **conhost.exe**, indicante il comando Ping TCP/IP.

3) Fare clic con il pulsante destro sul processo cmd.exe e selezionare Kill Process.

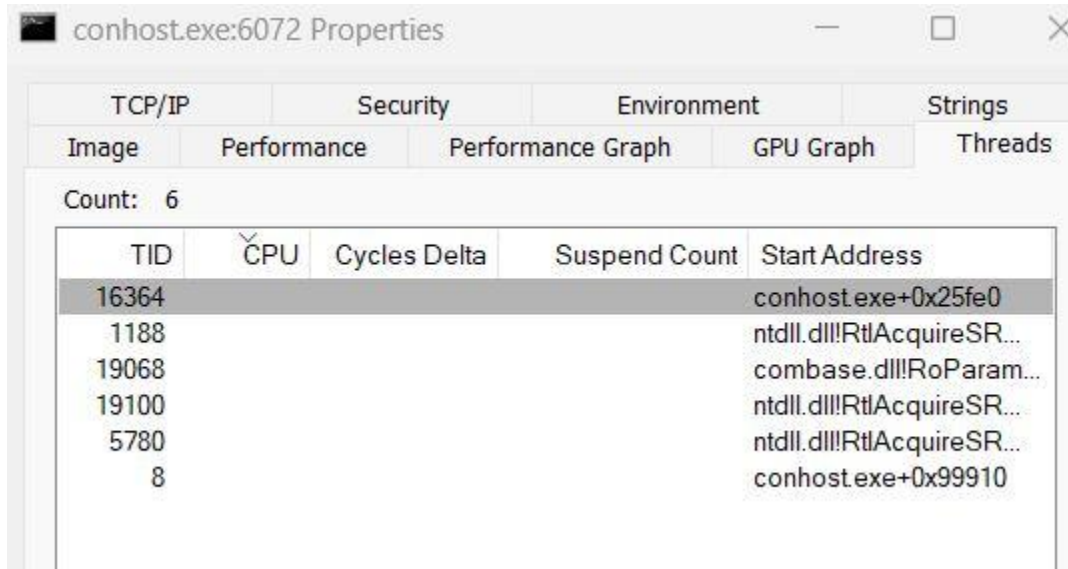
Cosa è successo al processo figlio conhost.exe?

cmd.exe		5.112 K	5.344 K	14084 Processore dei comandi di ...	Microsoft Corporation
conhost.exe		1.508 K	9.660 K	2840 Host finestra console	Microsoft Corporation

Chiudendo cmd con Kill Process, si è chiuso pure conhost.exe

- 4) Nella finestra di Process Explorer, fare clic con il pulsante destro su conhost.exe e selezionare Properties -> Threads.

Che tipo di informazioni sono disponibili nella finestra Proprietà?

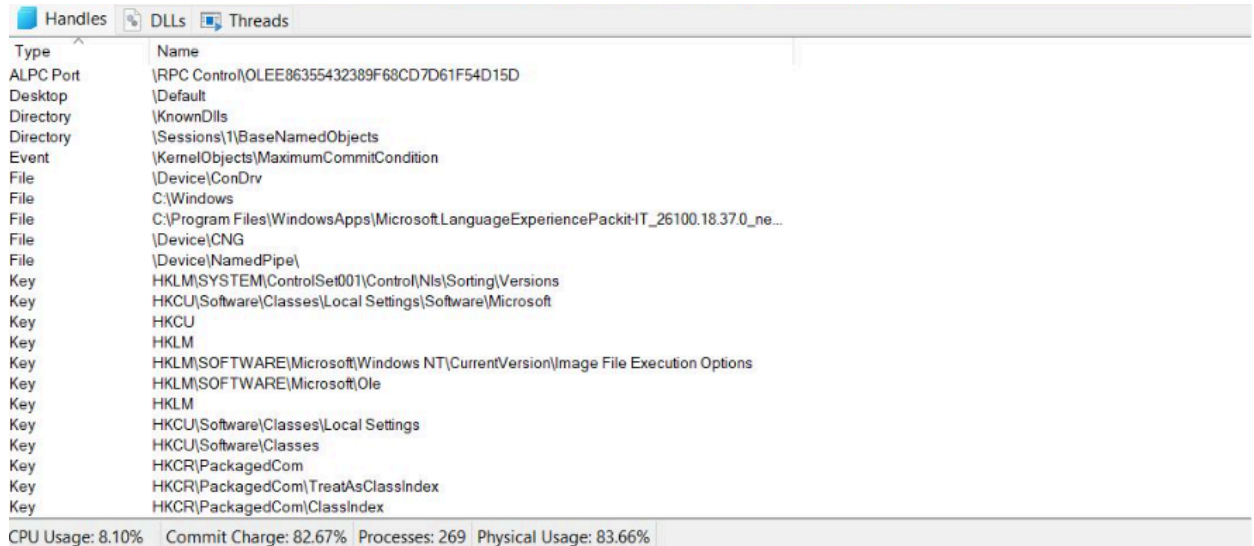


Nella finestra Proprietà sono disponibili diverse informazioni riguardo TCP/IP, Security, Environment, Strings, Image etc, come visibile dallo screen,

Ma in particolare sono presenti dettagli riguardo l'utilizzo della CPU, il numero di cicli della CPU utilizzati da un **thread** e quante volte questo thread è stato sospeso.

- 5) In Process Explorer, fare clic su View Visualizza) > selezionare Lower Pane View Vista Riquadro Inferiore) > Handles per visualizzare gli handle associati al processo conhost.exe.

Esaminare gli handle. A cosa puntano gli handle?



Type	Name
ALPC Port	\RPC Control\OLEE86355432389F68CD7D61F54D15D
Desktop	\Default
Directory	\KnownDlls
Directory	\Sessions\1\BaseNamedObjects
Event	\KernelObjects\MaximumCommitCondition
File	\Device\ConDrv
File	C:\Windows
File	C:\Program Files\WindowsApps\Microsoft.LanguageExperiencePack\IT_26100.18.37.0_ne...
File	\Device\CNG
File	\Device\NamedPipe\
Key	HKLM\SYSTEM\ControlSet001\Control\Nls\Sorting\Versions
Key	HKCU\Software\Classes\Local Settings\Software\Microsoft
Key	HKCU
Key	HKLM
Key	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options
Key	HKLM\SOFTWARE\Microsoft\Ole
Key	HKLM
Key	HKCU\Software\Classes\Local Settings
Key	HKCU\Software\Classes
Key	HKCR\PackagedCom
Key	HKCR\PackagedCom\TreatAsClassIndex
Key	HKCR\PackagedCom\ClassIndex

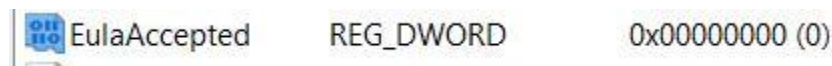
CPU Usage: 8.10% Commit Charge: 82.67% Processes: 269 Physical Usage: 83.66%

Gli handle visualizzabili puntano principalmente a file, console e Pipe.

- 6) Esplorazione del Registro di Windows.

Sulla chiave di registro **EulaAccepted**, cambiare il valore 1 in 0. Il valore 0 indica che l'EULA non è stato accettato.

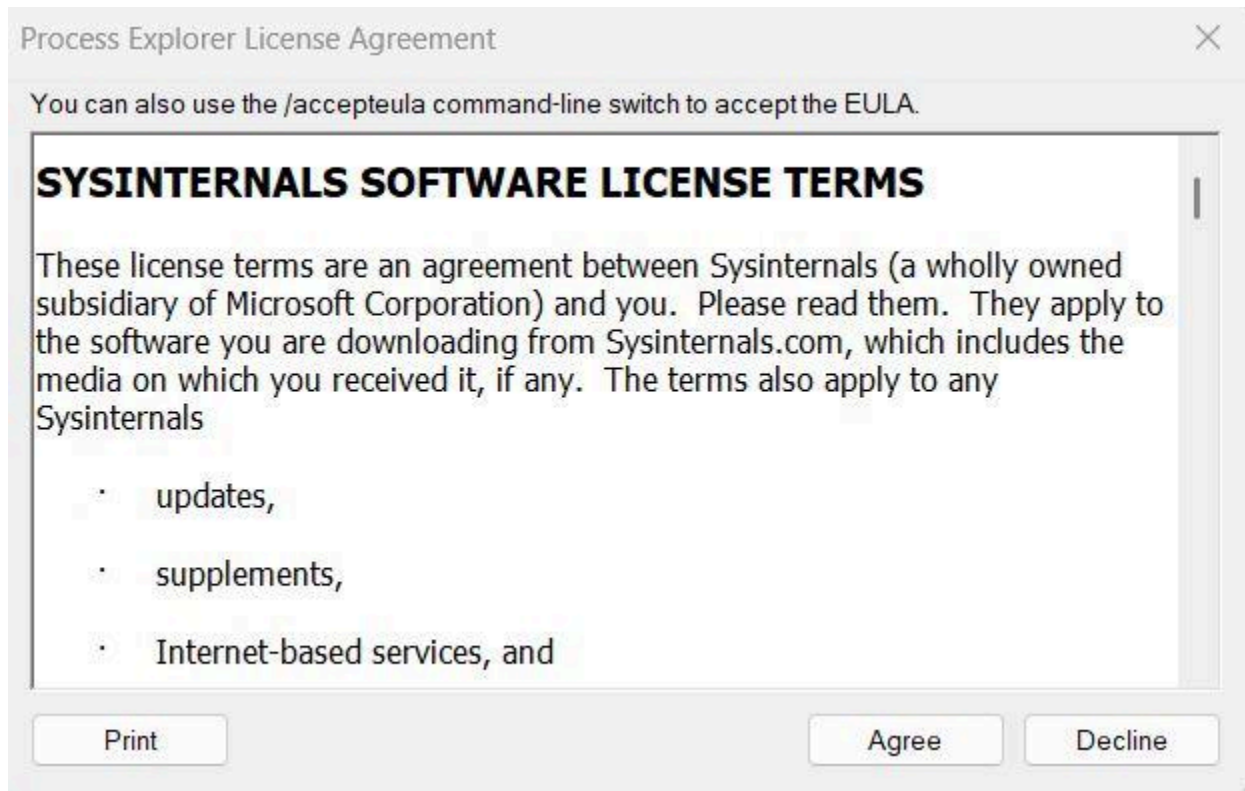
Qual è il valore per questa chiave di registro nella colonna Dati?



EulaAccepted	REG_DWORD	0x00000000 (0)
--------------	-----------	----------------

Il valore è 0.

Quando apri Process Explorer, cosa vedi?



Process Explorer una volta impostato il valore 0 in EulaAccepted, chiede di riaccettare l'Agreement, quindi come se non fosse stato accettato in precedenza.