UNIT3 S11/L1 - Esplorazione di Processi, Thread, Handle e Registro di Windows

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

l'applicazione è stata chiusa in maniera brutale.

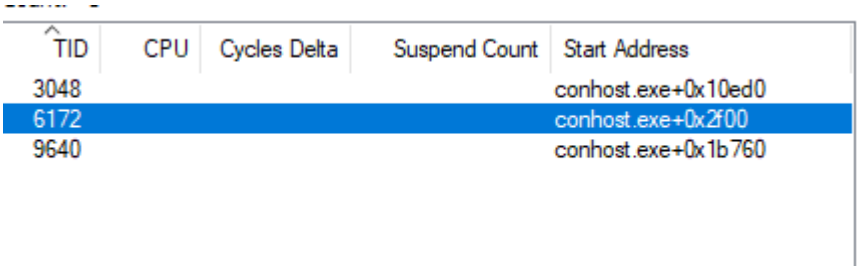
- **Avviare un altro processo. Navigare alla finestra del Prompt dei Comandi. Avviare un ping al prompt e osservare i cambiamenti sotto il processo cmd.exe. Cosa è successo durante il processo ping?**

appare un processo PING.EXE

- **Fare clic con il pulsante destro sul processo cmd.exe e selezionare Kill Process. Cosa è successo al processo figlio conhost.exe?**

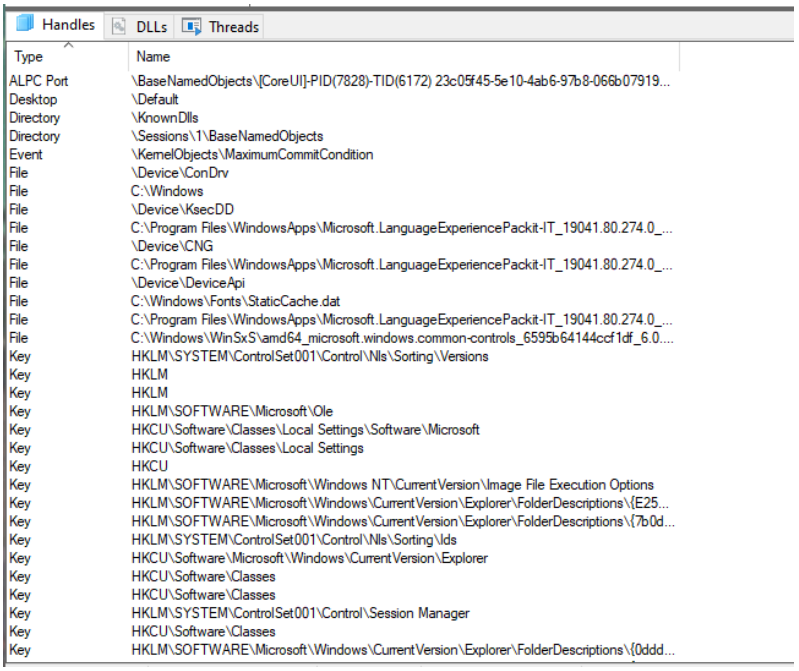
inevitabilmente chiudendo il processo padre "cmd.exe" verrà chiuso pure il processo figlio

- **Parte 2 Esplorazione di Thread e Handle. Che tipo di informazioni sono disponibili nella finestra Proprietà?**



TID	CPU	Cycles Delta	Suspend Count	Start Address
3048				conhost.exe+0x10ed0
6172				conhost.exe+0x2f00
9640				conhost.exe+0x1b760

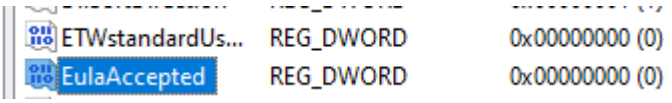
- **Esaminare gli handle. A cosa puntano gli handle?**



Handles | DLLs | Threads

Type	Name
ALPC Port	\BaseNamedObjects\[CoreUI]-PID(7828)-TID(6172) 23c05f45-5e10-4ab6-97b8-066b07919...
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\CNG
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
Key	HKLM
Key	HKLM
Key	HKLM\SOFTWARE\Microsoft\Ole
Key	HKCU\Software\Classes\Local Settings\Software\Microsoft
Key	HKCU\Software\Classes\Local Settings
Key	HKCU
Key	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options
Key	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{E25...
Key	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{7b0d...
Key	HKLM\SYSTEM\ControlSet001\Control\Nls\Sorting\Ids
Key	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer
Key	HKCU\Software\Classes
Key	HKCU\Software\Classes
Key	HKLM\SYSTEM\ControlSet001\Control\Session Manager
Key	HKCU\Software\Classes
Key	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{0ddd...

- **Cambiare il valore 1 in 0 per il dato Valore Value data. Il valore 0 indica che l'EULA non è stato accettato. Fare clic su OK per continuare. Qual è il valore per questa chiave di registro nella colonna Dati Data?**



- **Aprire Process Explorer. Navigare alla cartella in cui è stato scaricato SysInternals. Aprire la cartella SysInternalsSuite > Aprire procexp.exe. Quando apri Process Explorer, cosa vedi?**

Mi viene richiesto di accettare il SYSINTERNALS SOFTWARE LICENSE TERMS