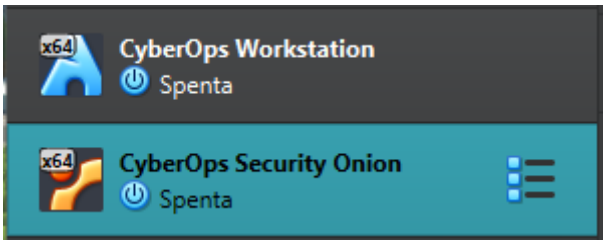
Esplorazione di Processi, Thread, Handle e Registro di Windows

1. installazione VMs:



Esplorazione di un processo attivo

Utilizzando la funzione `find window's process` dello strumento `procexp` e' possibile ottenere il processo di una finestra in esecuzione, in questo modo e' stato ottenuto il processo del web browser edge:

explorer.exe	1.03	37.272 K	108.848 K	4164 Windows Explorer	Microsoft Corporation
VBoxTray.exe	< 0.01	2.724 K	11.316 K	1768 VirtualBox Guest Additions Tr...	Oracle and/or its affiliates
ZoomIt64.exe		1.816 K	8.300 K	4396 Sysinternals Screen Magnifier	Sysinternals - www.sysinter...
msedge.exe	< 0.01	27.900 K	103.628 K	1232 Microsoft Edge	Microsoft Corporation
msedge.exe		1.968 K	7.484 K	1596 Microsoft Edge	Microsoft Corporation
msedge.exe		14.548 K	41.972 K	2792 Microsoft Edge	Microsoft Corporation
msedge.exe		7.896 K	24.968 K	2768 Microsoft Edge	Microsoft Corporation
msedge.exe		6.380 K	17.064 K	2940 Microsoft Edge	Microsoft Corporation
msedge.exe		21.736 K	77.752 K	1852 Microsoft Edge	Microsoft Corporation
msedge.exe		17.948 K	58.056 K	3284 Microsoft Edge	Microsoft Corporation
msedge.exe		12.536 K	27.588 K	4880 Microsoft Edge	Microsoft Corporation

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

La finestra si e' chiusa correttamente e senza alert o errori.

Apertura del CMD e ricerca del processo:

cmd.exe	4.060 K	4.184 K	1196 Windows Command Processor	Microsoft Corporation
conhost.exe	7.104 K	16.152 K	6772 Console Window Host	Microsoft Corporation

Dopo aver lanciato il comando `ping 192.168.0.1`:

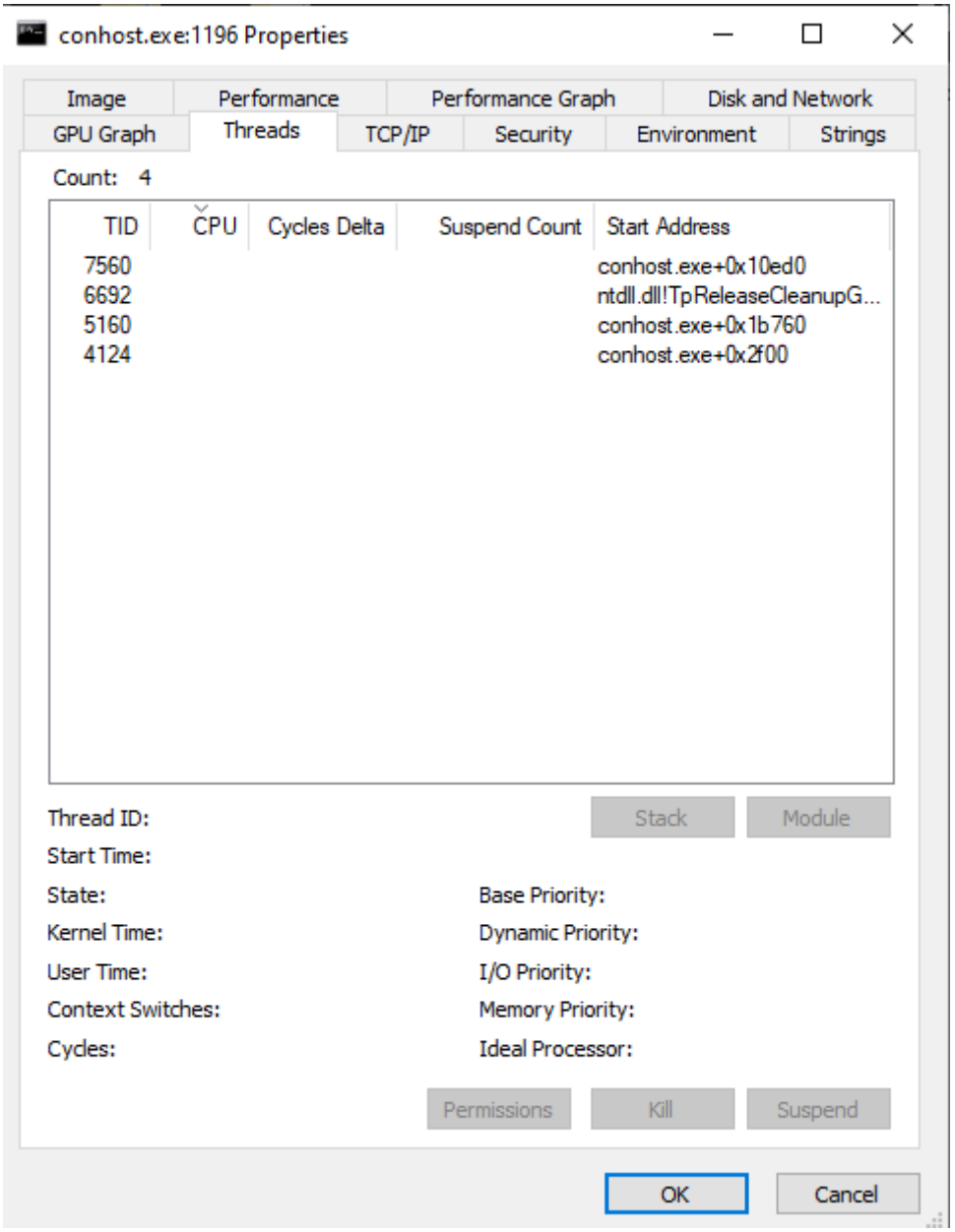
cmd.exe	< 0.01	2.436 K	4.708 K	1196 Windows Command Processor	Microsoft Corporation
conhost.exe	< 0.01	7.076 K	18.240 K	6772 Console Window Host	Microsoft Corporation
PING.EXE	< 0.01	856 K	3.880 K	2536 TCP/IP Ping Command	Microsoft Corporation

Cosa è successo durante il processo ping?

Come possiamo notare e' comparso il processo PING.EXE per poi scomparire dopo le normali 4 esecuzioni.

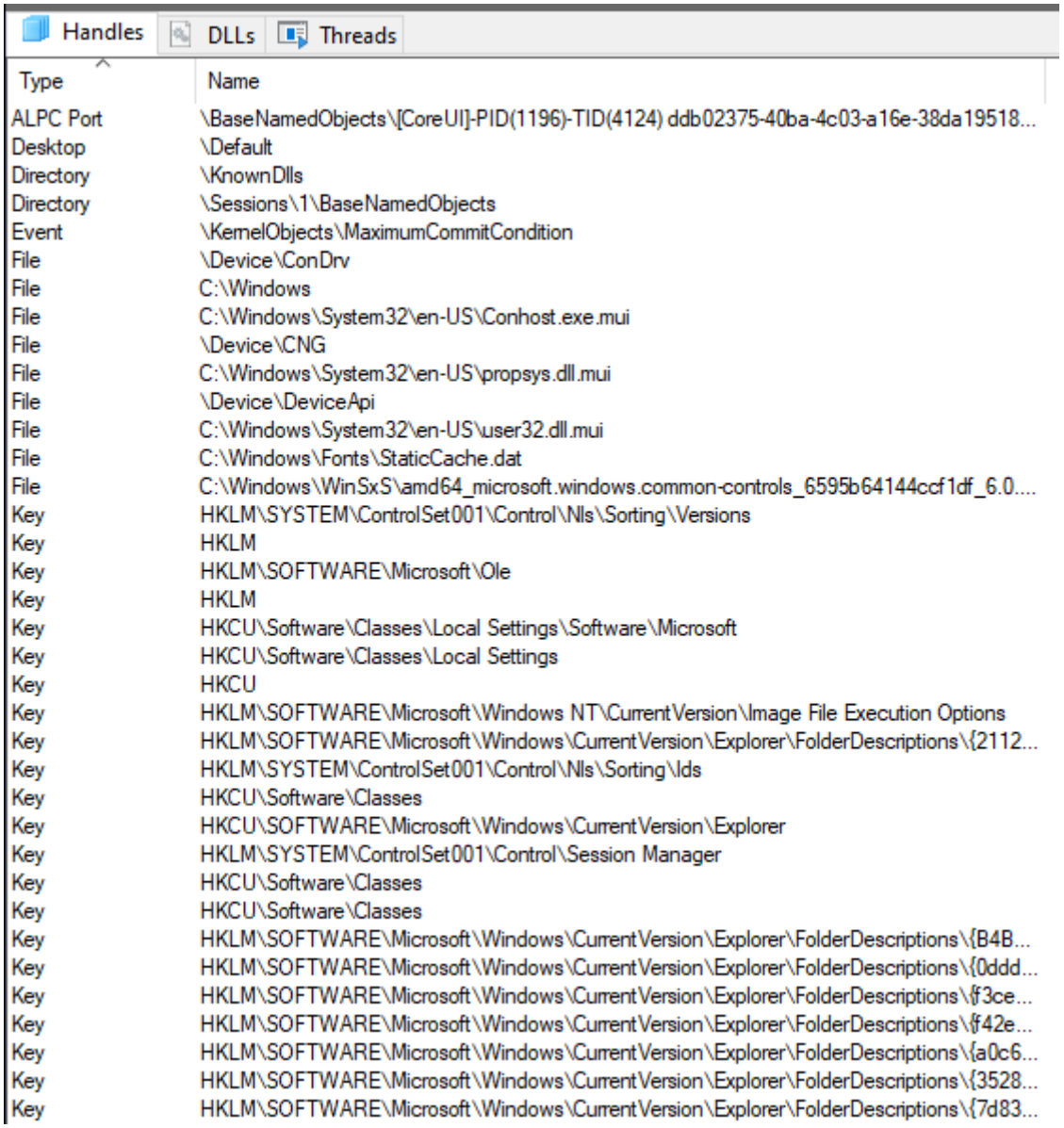
Cosa è successo al processo figlio conhost.exe?
E' stata richiesta la conferma di voler chiudere il processo, e selezionando "sì" il processo padre si e' chiuso insieme al processo figlio.

Proprieta' processo (scheda Threads):



Che tipo di informazioni sono disponibili nella finestra Proprietà?
Nella scheda threads possiamo notare informazioni come il numero di thread attivi, il thread ID.
Selezionando uno dei thread e' possibile ottenere informazioni come lo stato del thread, il tempo di esecuzione, informazioni su diverse priorita'.

Handles del processo `conhost.exe`:



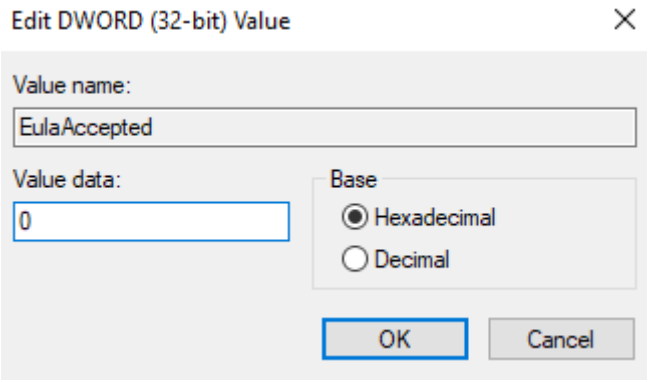
Handles | DLLs | Threads

Type	Name
ALPC Port	\BaseNamedObjects\[CoreUI]-PID(1196)-TID(4124) ddb02375-40ba-4c03-a16e-38da19518...
Desktop	\Default
Directory	\KnownDlls
Directory	\Sessions\1\BaseNamedObjects
Event	\KernelObjects\MaximumCommitCondition
File	\Device\ConDrv
File	C:\Windows
File	C:\Windows\System32\en-US\Conhost.exe.mui
File	\Device\CNG
File	C:\Windows\System32\en-US\propsys.dll.mui
File	\Device\DeviceApi
File	C:\Windows\System32\en-US\user32.dll.mui
File	C:\Windows\Fonts\StaticCache.dat
File	C:\Windows\WinSxS\amd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0....
Key	HKLM\SYSTEM\ControlSet001\Control\Nls\Sorting\Versions
Key	HKLM
Key	HKLM\SOFTWARE\Microsoft\Ole
Key	HKLM
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\{2112...
Key	HKLM\SYSTEM\ControlSet001\Control\Nls\Sorting\Ids
Key	HKCU\Software\Classes
Key	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer
Key	HKLM\SYSTEM\ControlSet001\Control\Session Manager
Key	HKCU\Software\Classes
Key	HKCU\Software\Classes
Key	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{B4B...
Key	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{0ddd...
Key	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{f3ce...
Key	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{f42e...
Key	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{a0c6...
Key	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{3528...
Key	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{7d83...

Esaminare gli handle. A cosa puntano gli handle?

Gli handle del processo puntano a diversi oggetti di sistema, tra cui File, chiavi di registro, il riferimento all'oggetto grafico per l'interfaccia (`type=Desktop`), Directory e eventi.

Re-impostazione del parametro EulaAccepted per Process Explorer:



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

`0x00000000 (0)`

Quando apri Process Explorer, cosa vedi?

Il software ci sta chiedendo di accettare l'EULA perche' abbiamo modificato il valore della chiave EulaAccepted.