LABORATORIO 17 FEBBRAIO 2025 S11-L1

Laboratorio:

Esplorazione di Processi, Thread, Handle e Registro di Windows

In questo laboratorio, completerai i seguenti obiettivi:

● Esplora i processi, i thread e gli handle utilizzando Process Explorer nella Sysinternals Suite.

● Utilizza il Registro di Windows per modificare un'impostazione.

https://itexamanswers.net/3-2-11-lab-exploring-processes-threads-handles-and-windowsregistry-answers.html

Nel compito odierno dobbiamo completare il laboratorio guidato relativo al link fornitoci.

Contents

PARTE 1: In questa parte dovremo esplorare i processi, ovvero i programmi e le applicazioni in esecuzione. Inizieremo un nuovo processo e lo osserveremo.

Passaggio 1: Scaricare la Suite Sysinternals che ci servirà per esplorare i processi. Successivamente al download, estraiamo i file

Part 1: Exploring Processes

In this part, you will explore processes. Processes are programs or applications in execution. You will explore the processes using Process Explorer in the Windows SysInternals Suite. You will also start and observe a new process.

Step 1: Download Windows SysInternals Suite.

a. Navigate to the following link to download Windows SysInternals Suite:

https://technet.microsoft.com/en-us/sysinternals/bb842062.aspx

b. After the download is completed, extract the files from the folder.

c. Leave the web browser open for the following steps.

Passiamo alla seconda parte in cui ci viene richiesto di estrarre i file dalla cartella compressa e aprire **procexp.exe** che mostrerà la lista dei processi correnti attivi. Trasciniamo l'icona della ricerca della finestra sul browser web che stiamo utilizzando.

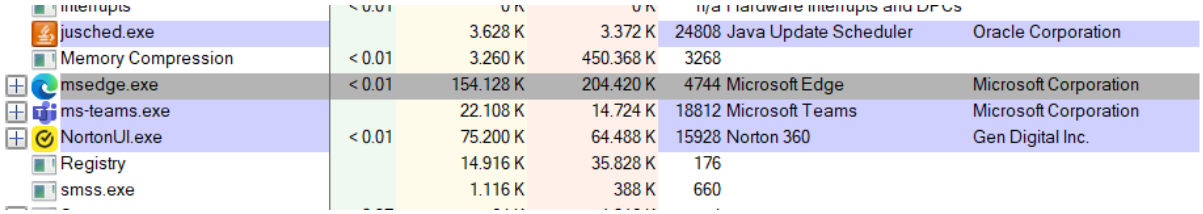
Step 2: Explore an active process.

a. Navigate to the SysinternalsSuite folder with all the extracted files.

b. Open **procexp.exe**. Accept the Process Explorer License Agreement when prompted.

c. The Process Explorer displays a list of currently active processes.

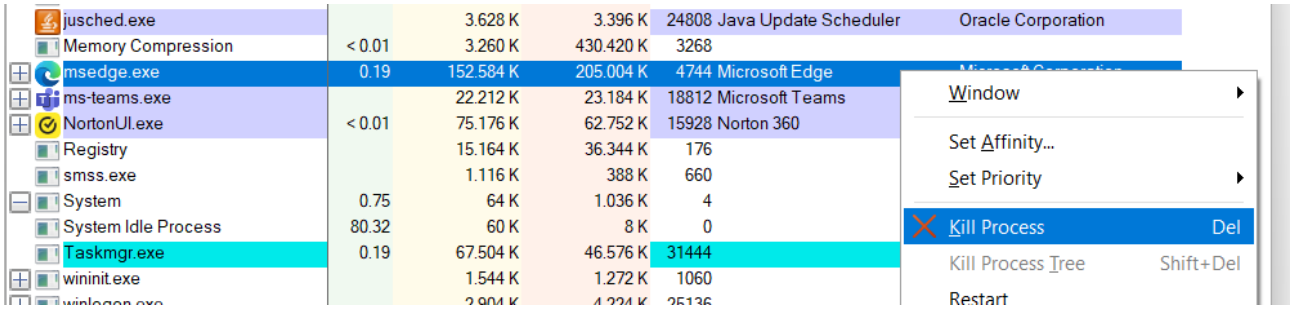
d. To locate the web browser process, drag the **Find Window's Process** icon into the opened web browser window. Microsoft Edge was used in this example.

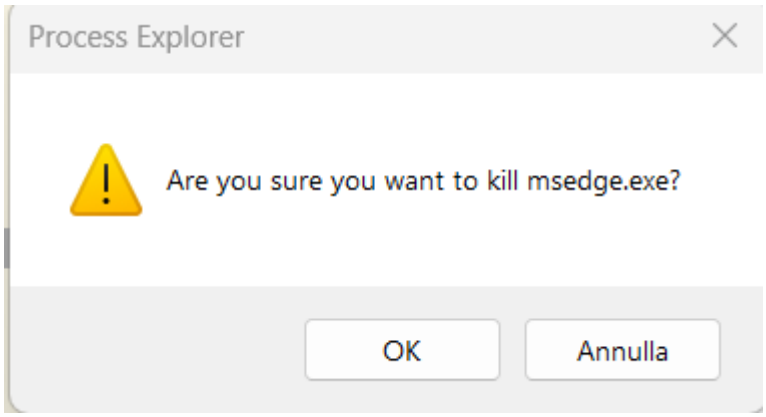


e. The Microsoft Edge process can be terminated in the Process Explorer. Right-click the selected process and select **Kill Process**. Click **OK** to continue.

What happened to the web browser window when the process is killed?

Facciamo click con il tasto destro sul processo e selezioniamo Kill Process. Questo farà si che il browser verrà chiuso.





Per il terzo step ci viene chiesto di aprire avviare un nuovo processo. Iniziamo aprendo il prompt dei comandi. Trasciniamo l'icona Processo della finestra trova nel prompt e individuiamolo in esplora processi. A questo punto notiamo che il processo prompt dei comandi è **cmd.exe** che è un processo figlio è **explorer.exe**. A sua volta il cmd.exe ha lui stesso un processo figlio che è **conhost.exe**.

Step 3: Start another process.

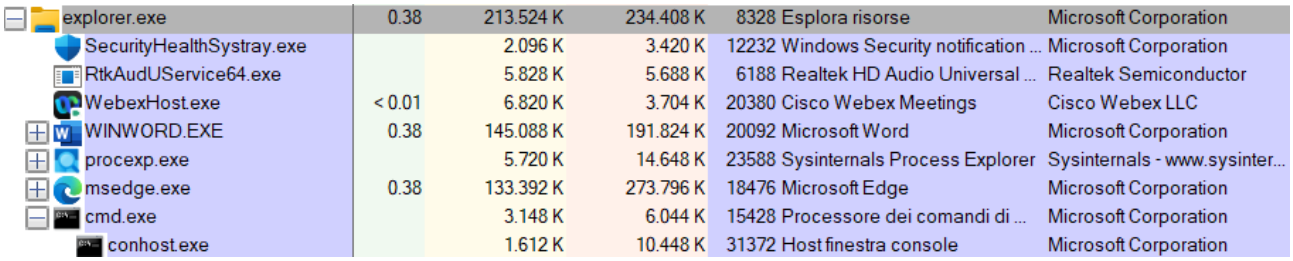
a. Open a Command Prompt. (**Start** > search **Command Prompt** > select **Command Prompt**)

b. Drag the **Find Window's Process** icon into the Command Prompt window and locate the highlighted Command Prompt process in Process Explorer.

c. The process for the Command Prompt is cmd.exe. Its parent process is explorer.exe process. The cmd.exe has a child process, conhost.exe.

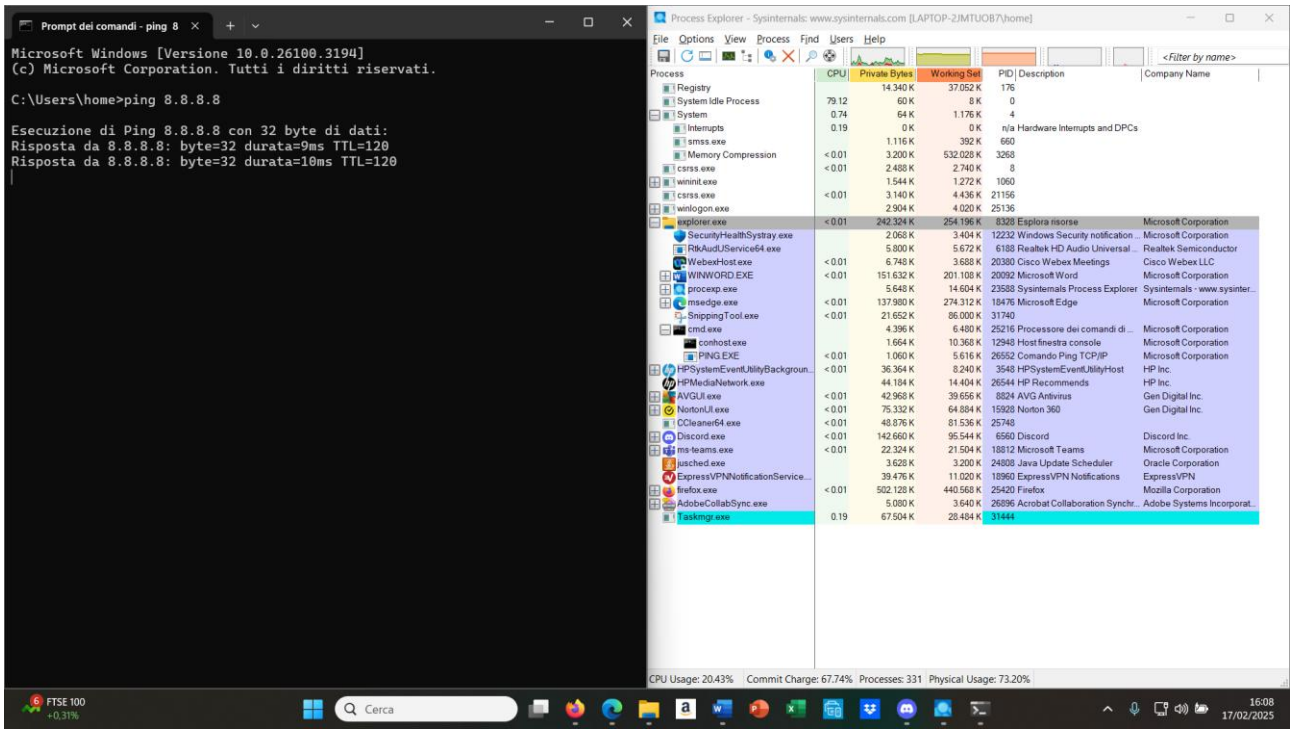
d. Navigate to the Command Prompt window. Start a ping at the prompt and observe the changes under the cmd.exe process.

What happened during the ping process?



explorer.exe	0.38	213.524 K	234.408 K	8328	Esplora risorse	Microsoft Corporation
SecurityHealthSystray.exe		2.096 K	3.420 K	12232	Windows Security notification ...	Microsoft Corporation
RtkAudUService64.exe		5.828 K	5.688 K	6188	Realtek HD Audio Universal ...	Realtek Semiconductor
WebexHost.exe	< 0.01	6.820 K	3.704 K	20380	Cisco Webex Meetings	Cisco Webex LLC
WINWORD.EXE	0.38	145.088 K	191.824 K	20092	Microsoft Word	Microsoft Corporation
procexp.exe		5.720 K	14.648 K	23588	Sysinternals Process Explorer	Sysinternals - www.sysinter...
msedge.exe	0.38	133.392 K	273.796 K	18476	Microsoft Edge	Microsoft Corporation
cmd.exe		3.148 K	6.044 K	15428	Processore dei comandi di ...	Microsoft Corporation
conhost.exe		1.612 K	10.448 K	31372	Host finestra console	Microsoft Corporation

Procediamo con un ping (per comodità lo effettueremo verso google e osserviamo la creazione di un nuovo processo figlio chiamato **PING.EXE** sotto il cmd.exe.



e. As you review the list of active processes, you find that the child process conhost.exe may be suspicious. To check for malicious content, right-click **conhost.exe** and select **Check VirusTotal**. When prompted, click **Yes** to agree to VirusTotal Terms of Service. Then click **OK** for the next prompt.

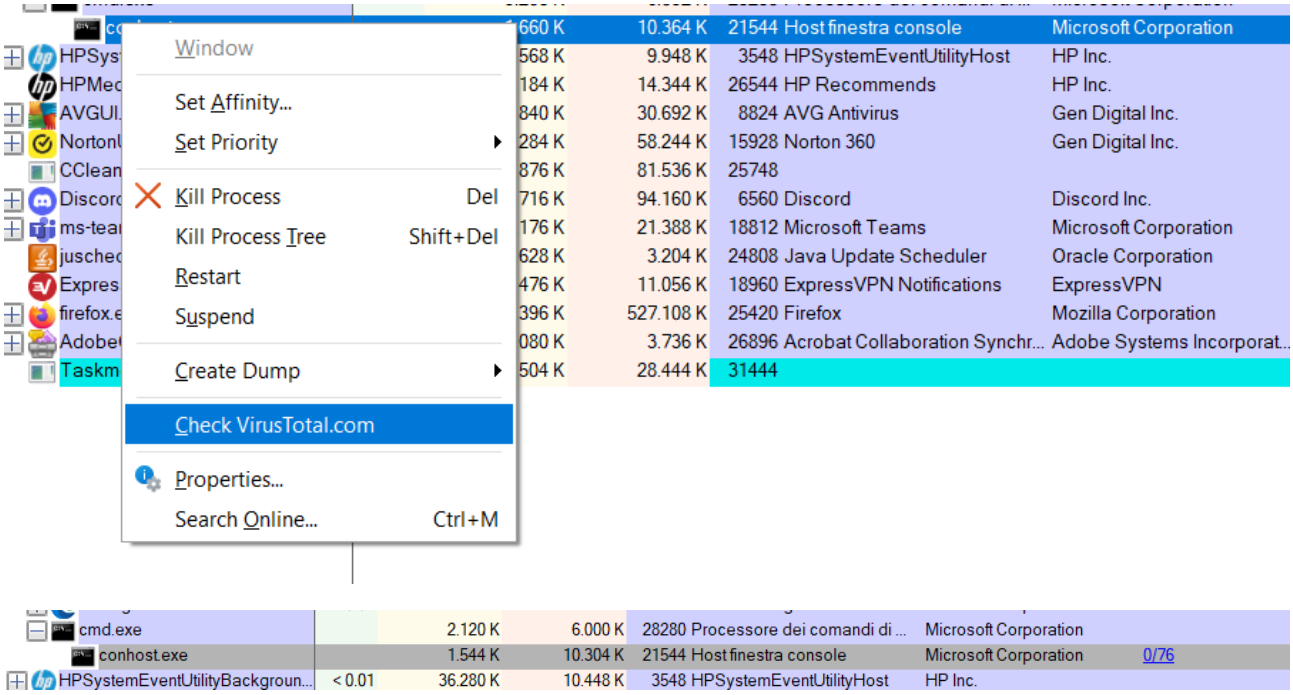
f. Expand the Process Explorer window or scroll to the right until you see the VirusTotal column. Click the link under the VirusTotal column. The default web browser opens with the results regarding the malicious content of conhost.exe.

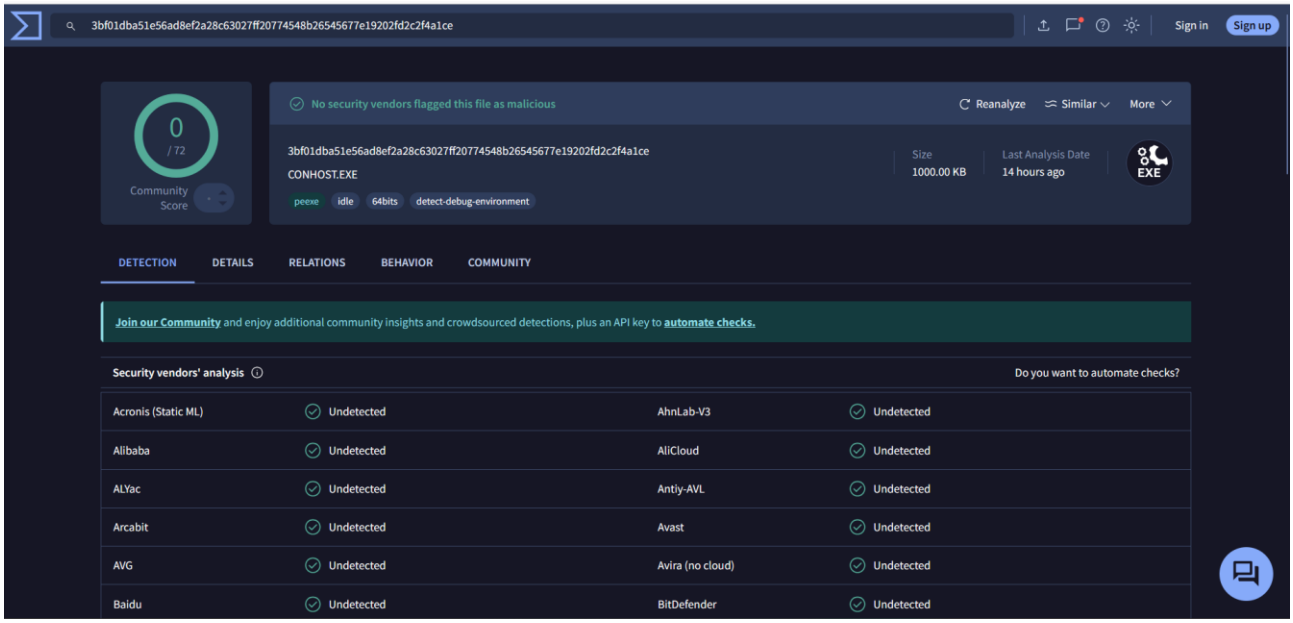
g. Right-click the cmd.exe process and select **Kill Process**.

What happened to the child process conhost.exe?

Esaminando la lista dei processi attivi si scopre che il conhost.exe potrebbe essere sospetto. Si procede quindi con una verifica di eventuali contenuti dannosi. Facciamo click con il tasto destro su conhost.exe e selezioniamo **Check VirusTotal**, accettiamo termini di servizio e andiamo avanti. Fatto ciò, scorriamo a destra fino alla colonna VirusTotal dove vedremo il risultato della scansione e con il tasto destro sullo stesso selezioniamo nuovamente Check

VirusTotal. L’ hash verrà scansionato e si aprirà sul nostro browser la schermata con il risultato.





Ora con il tasto destro sul processo cmd.exe selezioniamo Kill Process che chiuderà quello e anche il processo figlio conhost.exe.

PARTE 2: In questa parte esamineremo Threads e Handles. 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. Si userà Process Explorer (procexp.exe) in Windows SysInternals Suite per esplorare i thread e gli handle.

Part 2: Exploring Threads and Handles

In this part, you will explore threads and handles. Processes have one or more threads. A thread is a unit of execution in a process. A handle is an abstract reference to memory blocks or objects managed by an operating system. You will use Process Explorer (procexp.exe) in Windows SysInternals Suite to explore the threads and handles.

Step 1: Explore threads.

a. Open a command prompt.

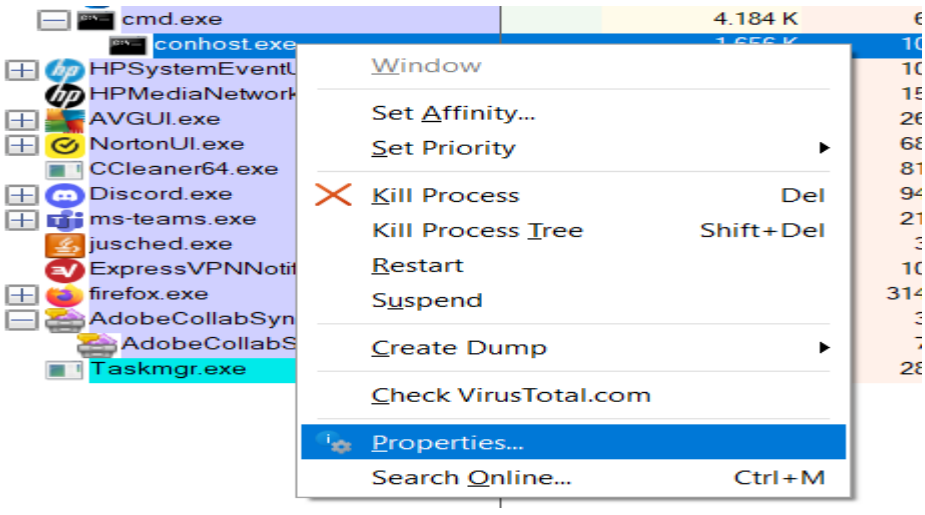
b. In Process Explorer window, right-click conhost.exe and Select **Properties…..** Click the **Threads** tab to view the active threads for the conhost.exe process. Click **OK** to continue if prompted by a warning dialog box.

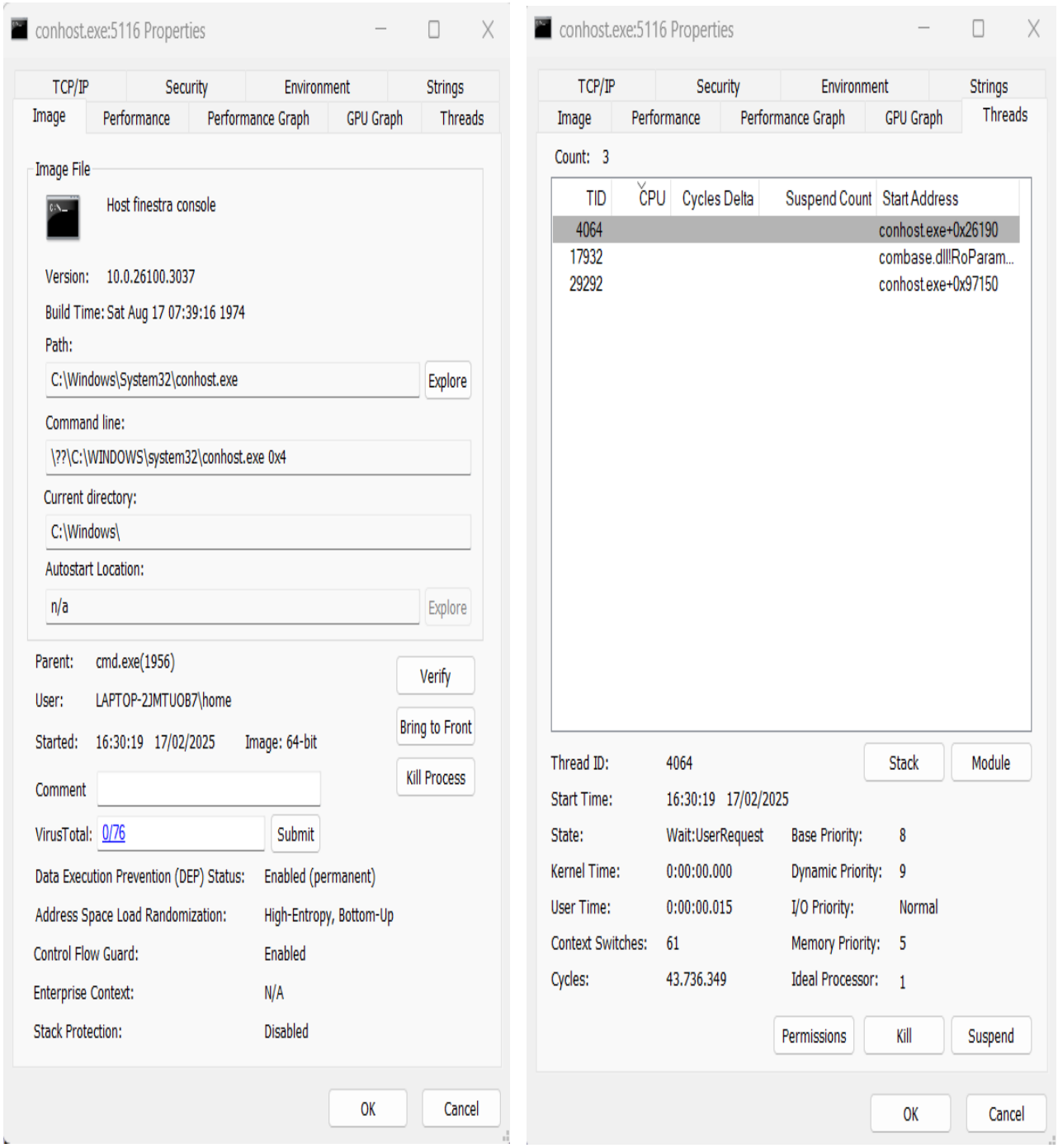
c. Examine the details of the thread.

What type of information is available in the Properties window?

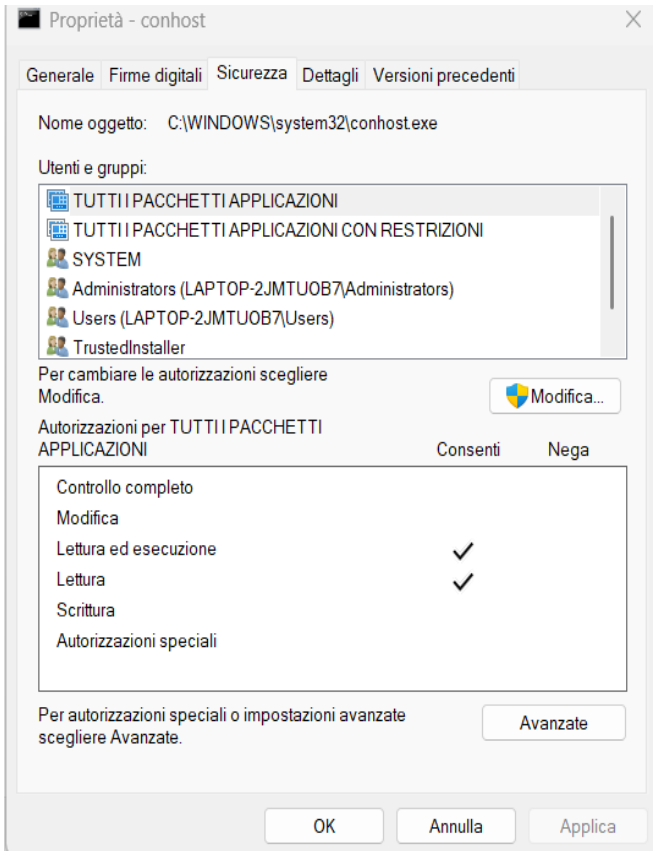
Passaggio 1: Esplorare i threads.

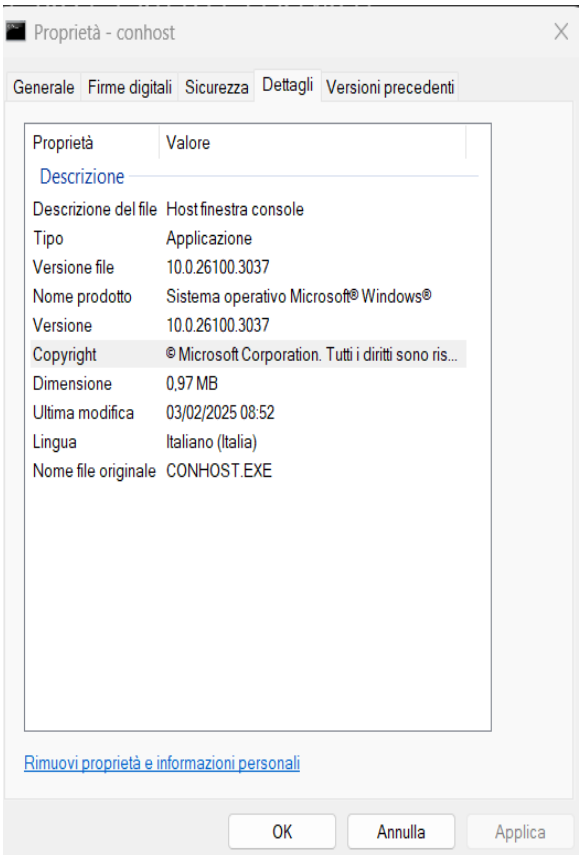
Apriamo il prompt dei comandi. Selezioniamo Properties con il tasto destro su conhost.exe, fare clic sulla scheda **Thread** per visualizzare i thread attivi per il processo conhost.exe. Esaminiamo i dettagli ottenuti.





Ci vengono restituite numerose informazioni sul processo e sui Thread attivi per lo stesso. Ad esempio il tempo di utilizzo dell' utente, quello del kernel, lo stato (in questo caso Wait) il suo TID, le priorità, la data e l'ora del suo avvio e il processore ideale. Cliccando su module possiamo controllare ulteriori informazioni tra cui quelle generali,la sicurezza, le firme digitali e i dettagli.





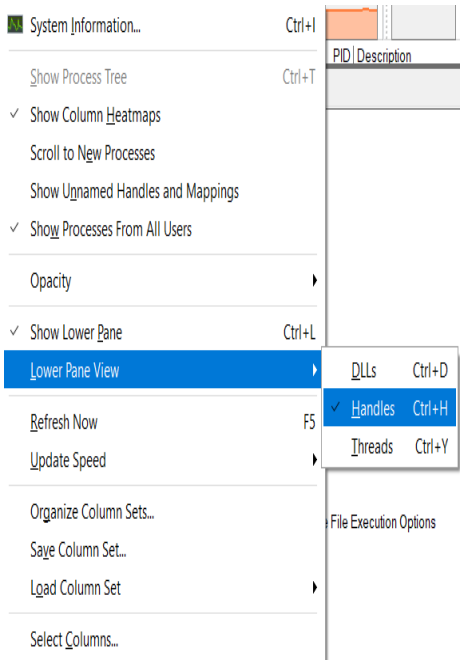
Passiamo all’esplorazione degli handles. Clicchiamo View e poi selezioniamo Lower Pane View e Handles per vedere quelli associati al processo conohost.exe

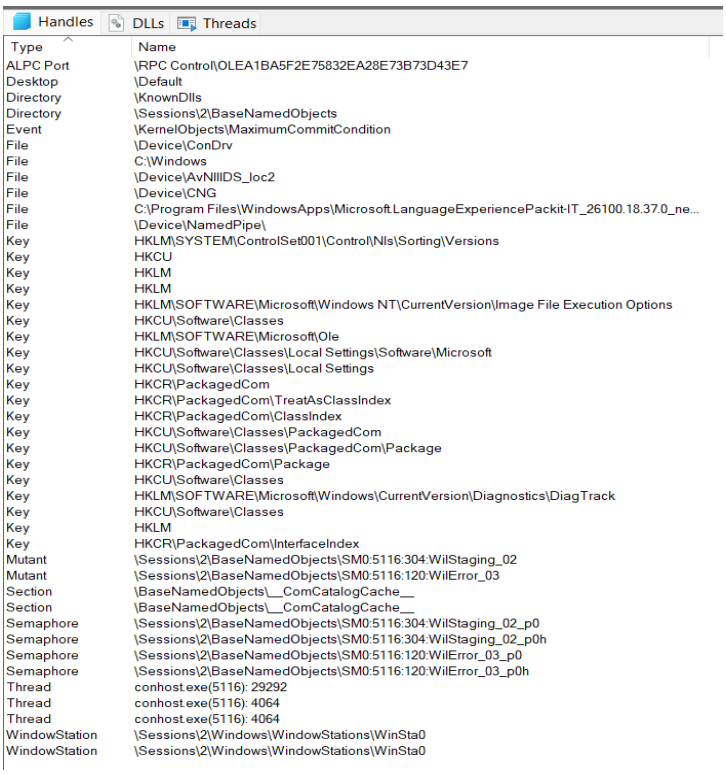
Step 2: Explore handles.

a. In the Process Explorer, click **View** > select **Lower Pane View** > **Handles** to view the handles associated with the conhost.exe process.

Examine the handles. What are the handles pointing to?

Possiamo vedere che gli handles puntano a file, chiavi del registro di sistema e thread.





PARTE 3: Esplorazione del registro di Windows.

Il registro di Windows è un database gerarchico che memorizza la maggior parte dei sistemi operativi e delle impostazioni di configurazione dell'ambiente desktop.

Part 3: Exploring Windows Registry

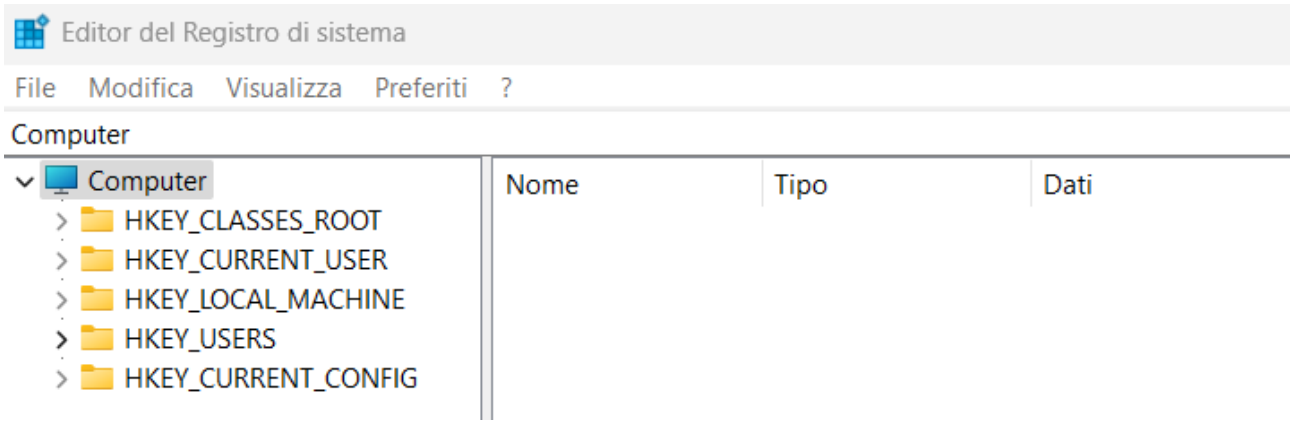
The Windows Registry is a hierarchical database that stores most of the operating systems and desktop environment configuration settings.

a. To access the Windows Registry, click **Start** > Search for **regedit** and select **Registry Editor**. Click **Yes** when asked to allow this app to make changes.

The Registry Editor has five hives. These hives are at the top level of the registry.

- HKEY_CLASSES_ROOT is actually the Classes subkey of HKEY_LOCAL_MACHINE\Software\. It stores information used by registered applications like file extension association, as well as a programmatic identifier (ProgID), Class ID (CLSID), and Interface ID (IID) data.
- HKEY_CURRENT_USER contains the settings and configurations for the users who are currently logged in.
- HKEY_LOCAL_MACHINE stores configuration information specific to the local computer.
- HKEY_USERS contains the settings and configurations for all the users on the local computer. HKEY_CURRENT_USER is a subkey of HKEY_USERS.
- HKEY_CURRENT_CONFIG stores the hardware information that is used at bootup by the local computer.

Per accedere al registro clicchiamo start, cerchiamo **regedit** e selezioniamo **Registry Editor**



b. In a previous step, you had accepted the EULA for Process Explorer. Navigate to the EulaAccepted registry key for Process Explorer.

Click to select Process Explorer in **HKEY_CURRENT_USER > Software > Sysinternals > Process Explorer**. Scroll down to locate the key **EulaAccepted**. Currently, the value for the registry key EulaAccepted is 0x00000001(1).

c. Double-click **EulaAccepted** registry key. Currently the value data is set to 1. The value of 1 indicates that the EULA has been accepted by the user.

d. Change the **1** to **0** for Value data. The value of 0 indicates that the EULA was not accepted. Click **OK** to continue.

What is value for this registry key in the Data column?

A questo punto dobbiamo passare alla chiave del Registro di sistema EulaAccepted per Process Explorer. Fare clic per selezionare Esplora processi in **HKEY_CURRENT_USER > Software > Sysinternals > Esplora processi**. Scorrere verso il basso per individuare la chiave **EulaAccepted**. Attualmente, il valore per la chiave del Registro di sistema EulaAccepted è 0x00000001(1).

Fare doppio click e modificare il valore da 1(accettato) a 0 (non accettato) e confermare con Ok.

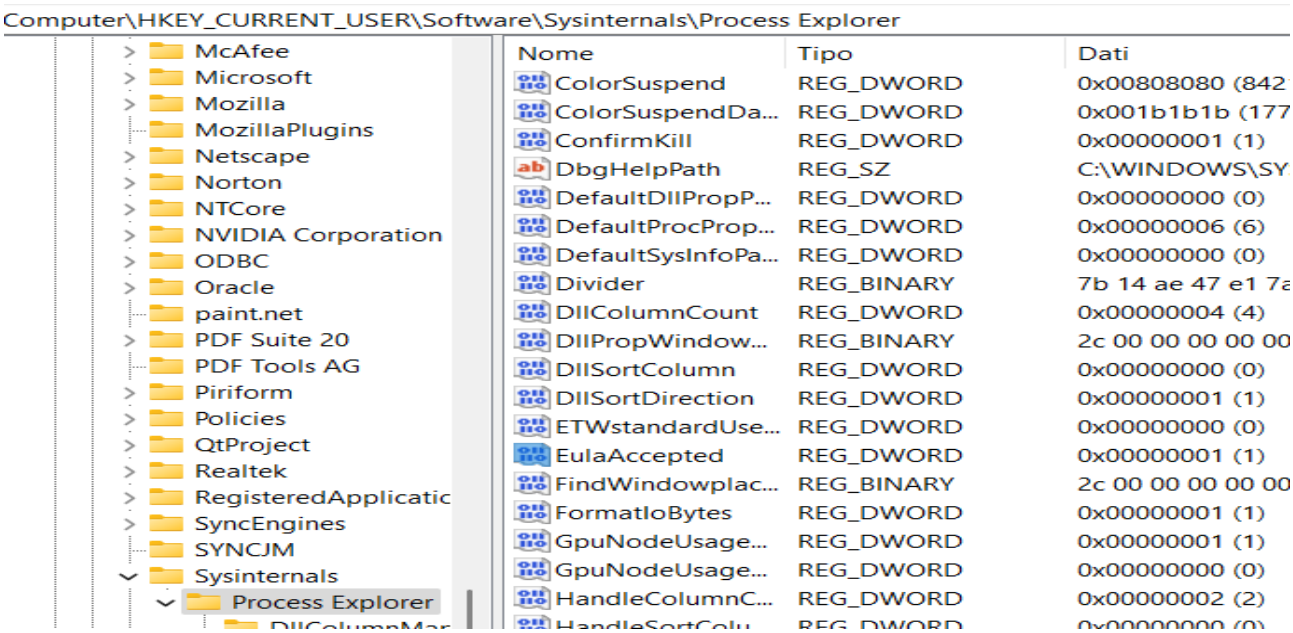
b. In a previous step, you had accepted the EULA for Process Explorer. Navigate to the EulaAccepted registry key for Process Explorer.

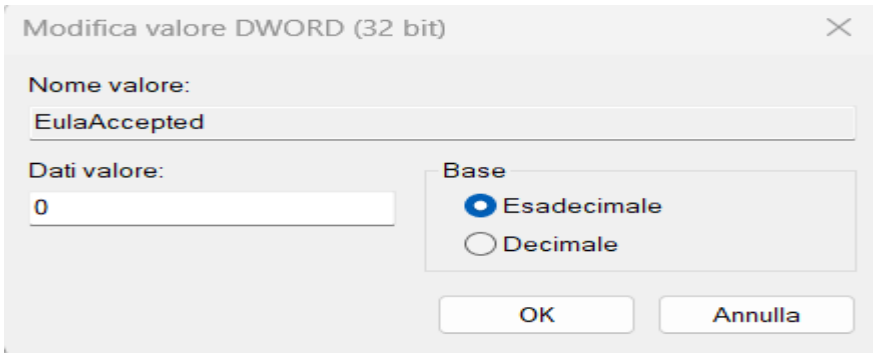
Click to select Process Explorer in **HKEY_CURRENT_USER > Software > Sysinternals > Process Explorer**. Scroll down to locate the key **EulaAccepted**. Currently, the value for the registry key EulaAccepted is 0x00000001(1).

c. Double-click **EulaAccepted** registry key. Currently the value data is set to 1. The value of 1 indicates that the EULA has been accepted by the user.

d. Change the **1** to **0** for Value data. The value of 0 indicates that the EULA was not accepted. Click **OK** to continue.

What is value for this registry key in the Data column?





Il valore per questa chiave di registro di sistema nella colonna Data è ora 0x00000000(0)

e. Open the **Process Explorer**. Navigate to the folder where you have downloaded SysInternals. Open the folder **SysInternalsSuite** > Open **procexp.exe.**

When you open the Process Explorer, what did you see?

Aprendo Process Explorer e navigando nella cartella di download di SysInternals apriamo la cartella e apriamo **procexp.exe**, il risultatò sarà l'apertura della finestra di dialogo Contratto di licenza Process Explorer.