Lab 2.1.2.10 – Exploring Processes, Threads, Handles, and Windows Registry

This lab has been updated for use on NETLAB+.
www.netdevgroup.com

Objectives

In this lab, you will explore the processes, threads, and handles using Process Explorer in the SysInternals Suite. You will also use the Windows Registry to change a setting.

Part 1: Exploring Processes

Part 2: Exploring Threads and Handles

Part 3: Exploring Windows Registry

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.

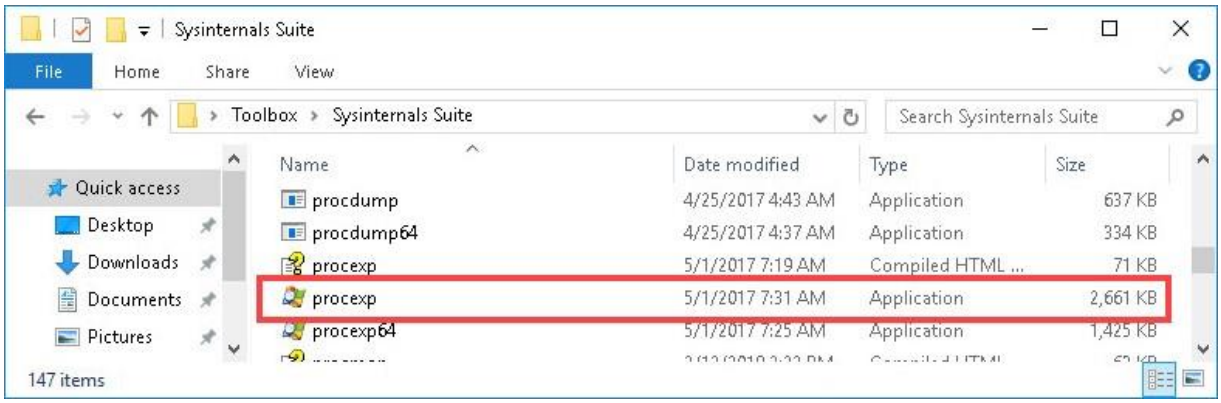
Step 1: Explore an active process.

a. Access the **WinClient** machine. Unlock the machine by clicking on the drop-down arrow for that specific machine's tab and select **Send CTRL+ALT+DEL**.

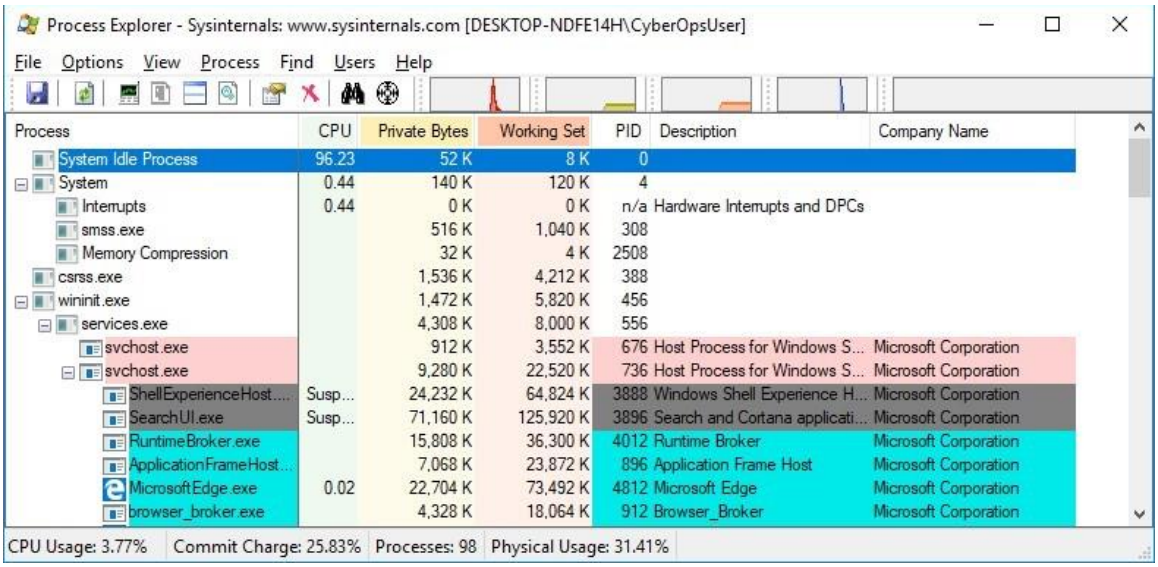
b. Login as the `administrator` using `cyberops` as the password.

c. Navigate to the **Toolbox > Sysinternals Suite** folder located on the *Desktop*.

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

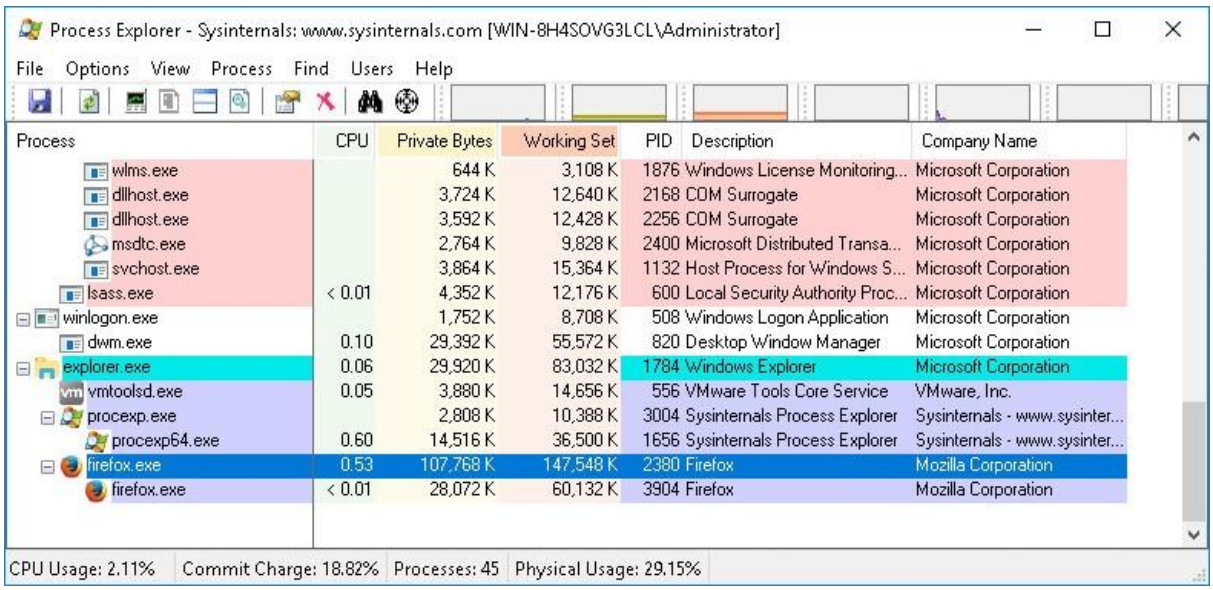


e. The *Process Explorer* displays a list off currently active processes.



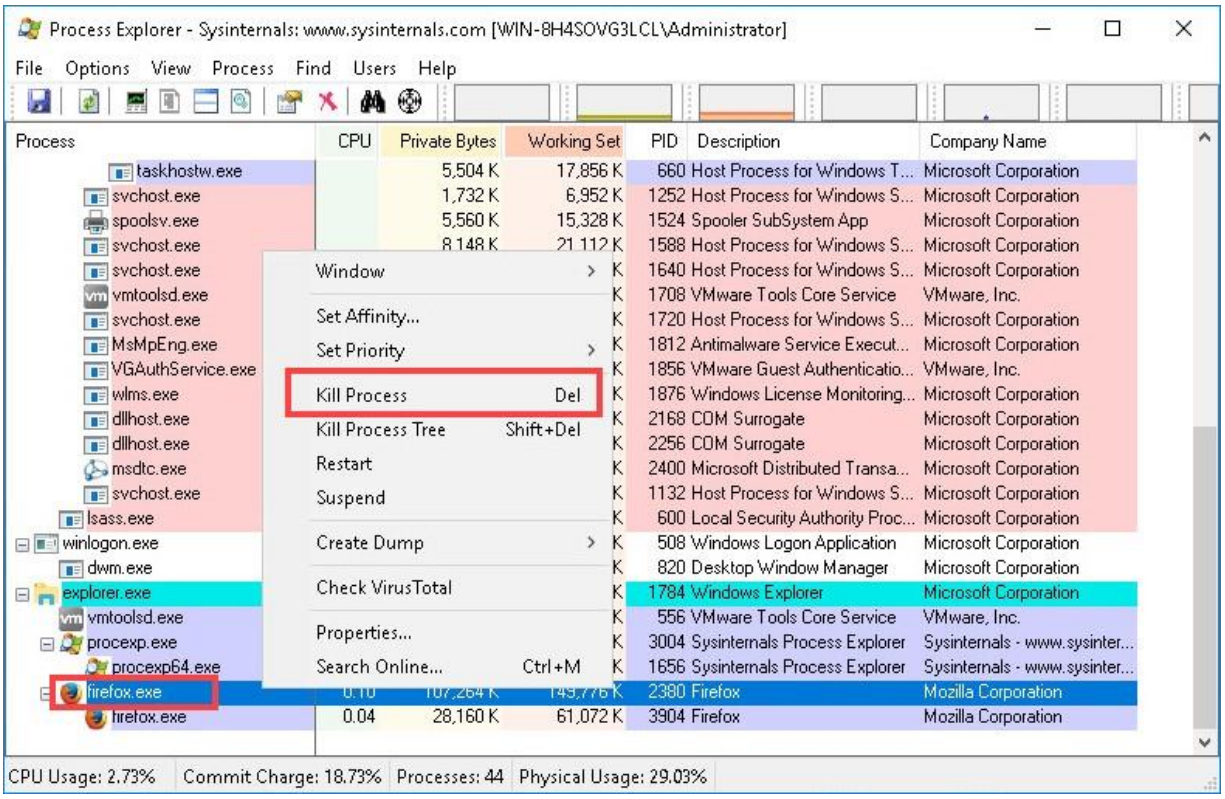
f. Launch the **Mozilla Firefox** web browser and leave it open in the background. Change focus to the **Process Explorer**.

g. To locate the web browser process, drag the **Find Window's Process** icon ( ) into the opened web browser window.



Make sure that when using the *Find Window's Process* feature that the *Process Explorer* window is in the foreground and that the *Mozilla Firefox* web browser is opened in the background. Using this feature on the toolbar icons will not accurately locate the intended object.

h. The *Mozilla Firefox* process can be terminated in the *Process Explorer*. Right-click the selected process and select **Kill Process**. When prompted, select **OK** to confirm.



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

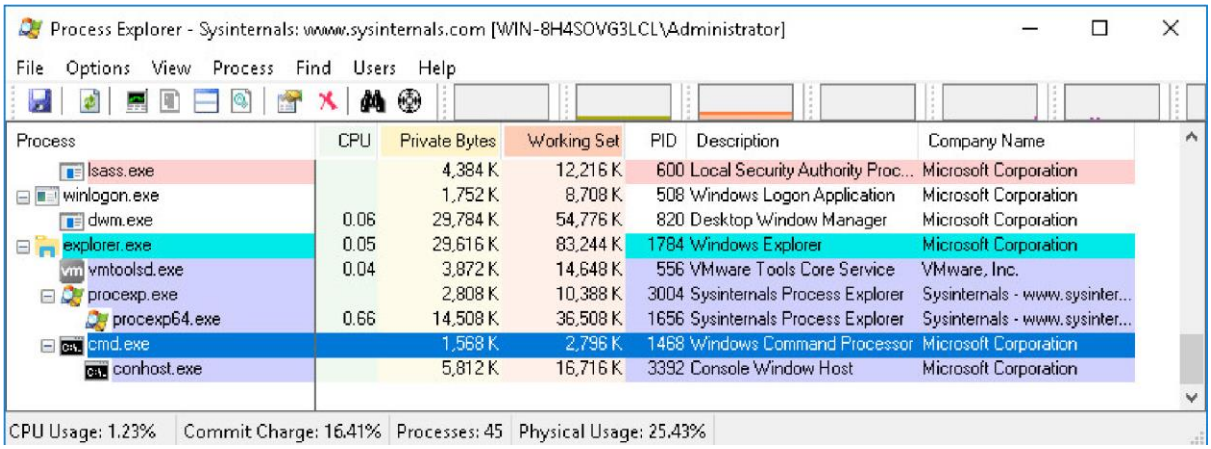
When the wed browser window when the process is killed it will automatically closed.

Step 2: 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 opened Command Prompt window and locate the highlighted *Command Prompt* process in *Process Explorer*.

c. Notice 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. Change focus to the **Command Prompt** window. Ping the local gateway at *192.168.0.1* and observe the changes under the *cmd.exe* process.

What happened during the ping process?

The Ping Process found that the local gateway isn't recognized. Under the cmd.exe file conhost.exe is listed.

If a process is found to be suspicious, you may right-click the process and use the *Check VirusTotal* feature. With an active internet connection, this feature will help detect whether a process has malicious content.

e. Right-click the cmd.exe process and select **Kill Process**. When prompted, click **OK**. What happened to the child process *conhost.exe*?

While in kill cmd.exe process, the child process conhost.exe will be deleted and window associated with cmd will close.

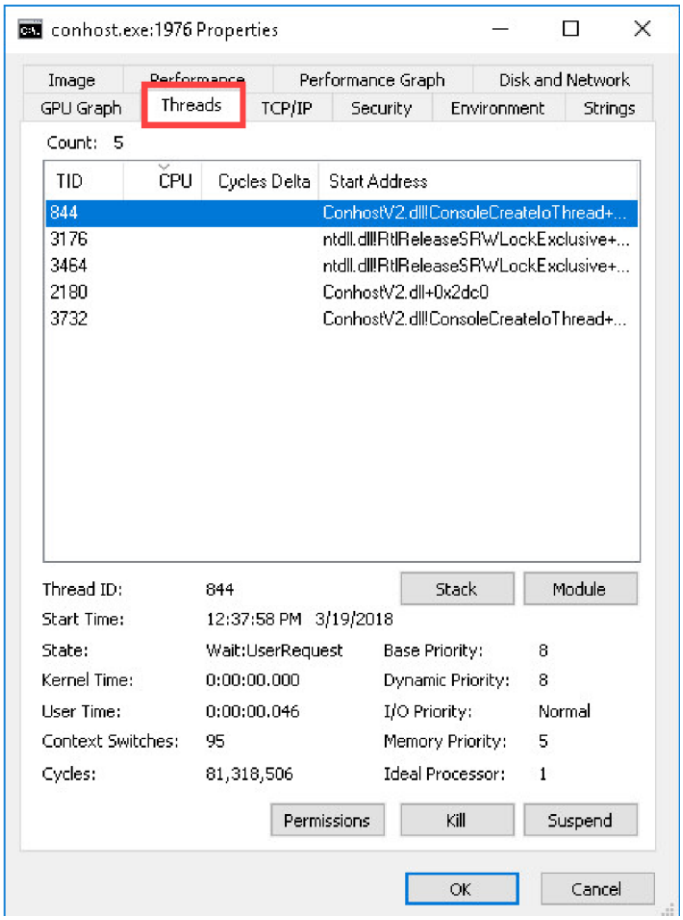
Part 2: Exploring Threads and Handles

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. If prompted with a warning, click **OK** to continue.



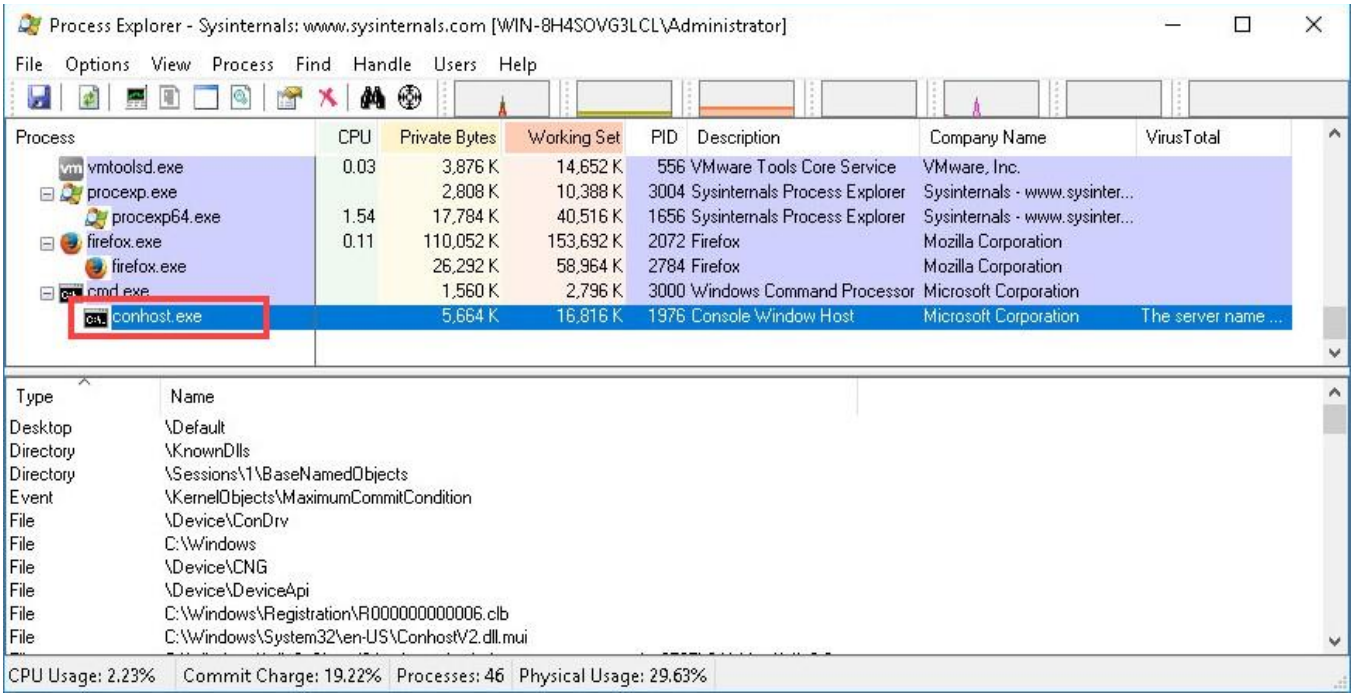
c. Examine the details of the thread. What type of information is available in the *Properties* window?

The information available about thread in properties windows are Performance, Security, Environment and strings.

d. Click **Cancel** to exit the properties window.

Step 2: Explore handles.

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



Examine the handles. What are the handles pointing to?

The handles are pointing to threads and files.

b. Close the **Process Explorer** window.

Part 3: Exploring Windows Registry

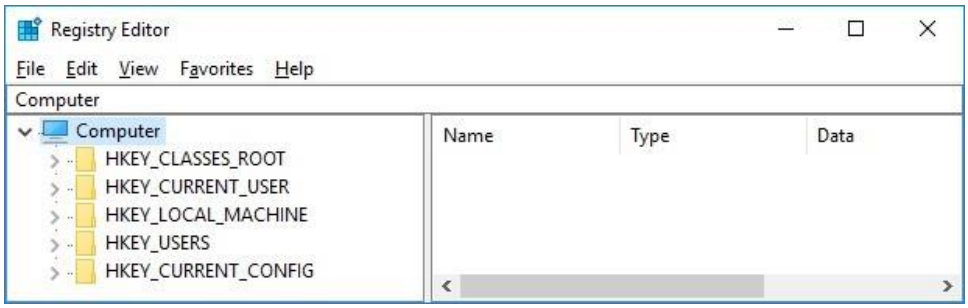
The *Windows Registry* is a hierarchical database that stores most of the operating systems and desktop environment configuration settings. In this part, you will

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

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

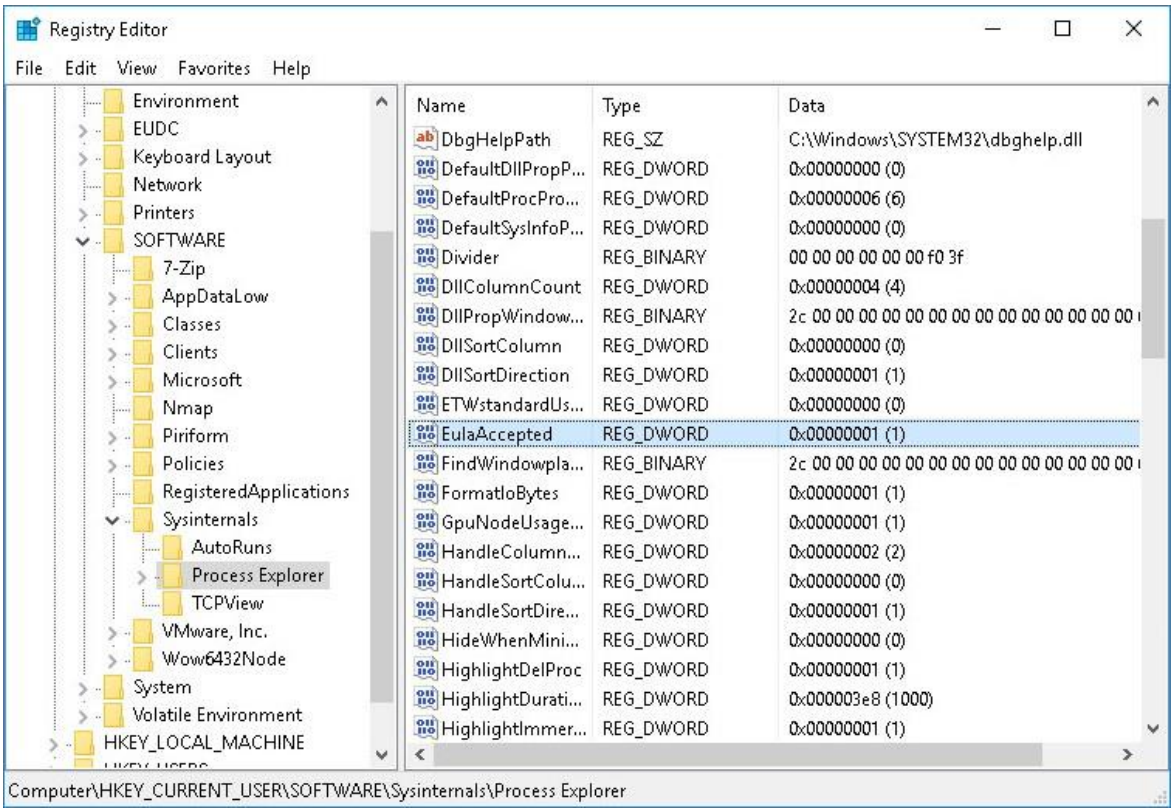
- *HKEY_CLASSES_ROOT* is actually the *Classes* subkey of *HKEY_LOCAL_MACHINE\Software*. It stores information used by registered applications like file extension association, as well as a programmatic identifier (*ProgID*), *Class ID* (*CLSID*), and *Interface ID* (*IID*) data.
- *HKEY_CURRENT_USER* 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.

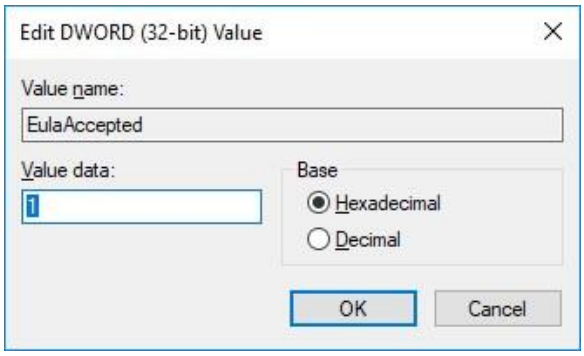


b. In a previous step, you had accepted the *EULA* for *Process Explorer*. Navigate to the *EulaAccepted* registry key for *Process Explorer*.

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?

0*00000000(0)

e. Navigate to the **Toolbox > Sysinternals Suite** folder. Double-click **procexp.exe** to launch **Process Explorer**.

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

When I the opened the process explorer it shows license agreement box.