Sysinternals Process Explorer

by Sid Paskowitz 5/2/2017

The information in this document is based on my understanding of Process Explorer and my use of it. Best if used by techies. Please note the information and displays below are subject to update or change and were applicable when this document was written. All the actions and displays were created using a 64-bit Windows 10 computer. Please send comments or suggestions for improving this document to wvcomputerclub@gmail.com.

*****

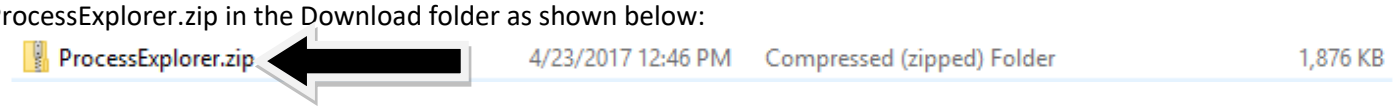
The following instructions describe the process for installing and running Sysinternals Process Explorer on a personal computer (PC). I have found Process Explorer to be a handy tool when, due to something I have done or when something happens unexpectedly, I suspect something unwanted is happening on my computer. When that happens, I run Process Explorer from my taskbar to determine if a virus is running on my computer.

Process Explorer is different from other anti-malware programs. Programs such as Malwarebytes and Windows Defender scan the computer's storage drive(s) to determine if malicious code is embedded on a drive. Process Explorer takes a "snapshot" of the code running on the computer and sends that "snapshot" to multiple reviewers to see if any reviewer finds any segment of the running code to be malicious or questionable. That process is quick and efficient, but it only displays a problem when malicious code is running when the "snapshot" is taken and will not show if malicious code is hiding elsewhere on the computer. When malicious code is found, Process Explorer may provide help for correcting the problem. I run Process Explorer from my taskbar because it is always accessible at the bottom of my computer screen.

Installation

The download site for Process Explorer is https://technet.microsoft.com/en-us/sysinternals/processexplorer.aspx as shown in the following display. Left-click on the download link (see arrow below) to download the program.

The downloaded file is a zipped file that can be opened (unzipped) by left-clicking (or double-left-clicking) on the file name ProcessExplorer.zip in the Download folder as shown below:



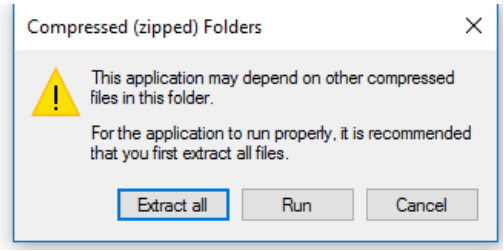
When I unzipped the file, it created a Process Explorer folder in my Documents folder:

When I opened the Process Explorer folder I got the following display:

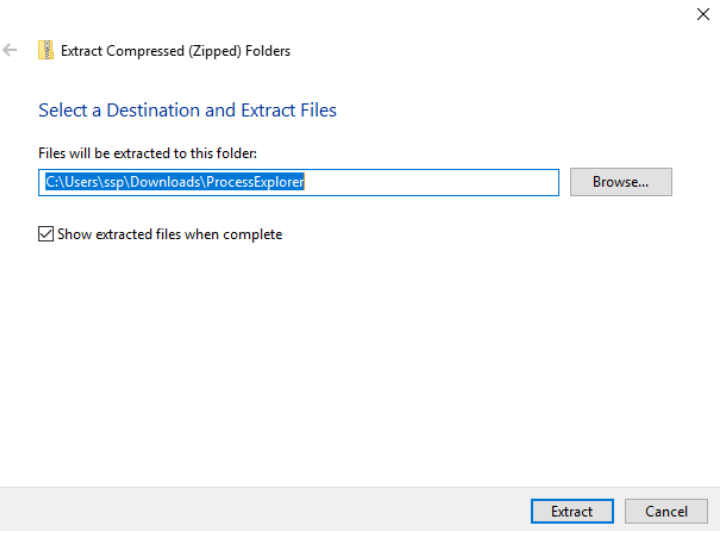
Name	Type	Compressed size	Password ...	Size	Ratio	Date modified
Eula.txt	Text Document	4 KB	No	8 KB	59%	3/3/2016 8:44 PM
procexp.chm	Compiled HTML Help file	64 KB	No	71 KB	11%	2/2/2017 11:32 AM
procexp.exe	Application	1,178 KB	No	2,648 KB	56%	2/2/2017 11:45 AM
procexp64.exe	Application	632 KB	No	1,419 KB	56%	2/2/2017 11:39 AM

It was not clear which .exe application file I should click on, so I chose the one with the larger size in hope of it having more content and capability. It is also possible that the file procexp64.exe is only to be used on 64-bit PCs, so to be on the safe side for all users, I chose procexp.exe as the preferred application.

When I clicked on the larger procexp.exe file name, I got the following display, and based on its recommendation, I clicked in the box to Extract all:

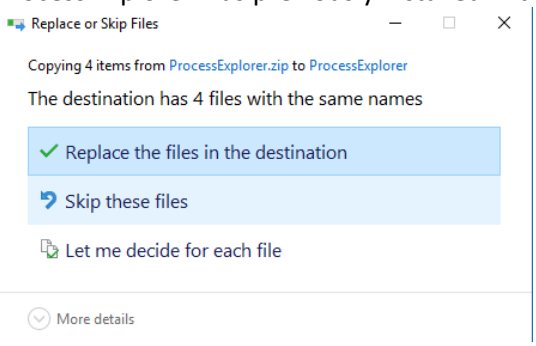


I then got the following display that asked where I wanted to put the extracted files.

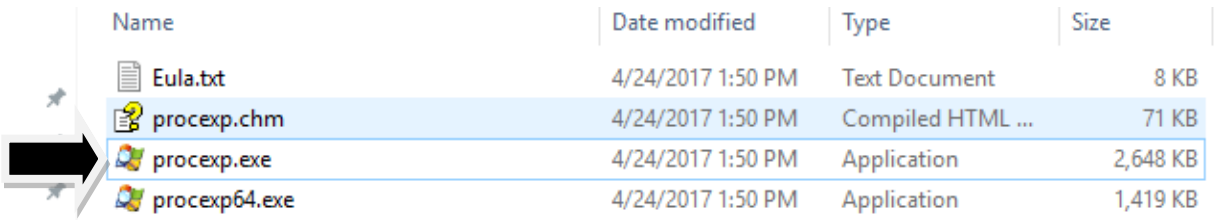


I could have changed the destination or browsed for a different destination, but I made a note about the destination selected for use as explained below, and I clicked in the Extract box.

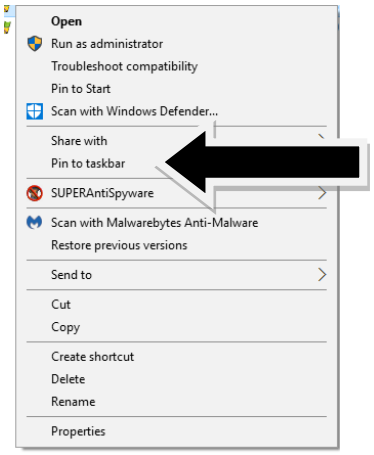
Process Explorer was previously installed in the selected destination and I got the following display:



To get the latest file versions, I selected (left-clicked on) the choice to Replace the files in the destination and got the following display in the destination folder:



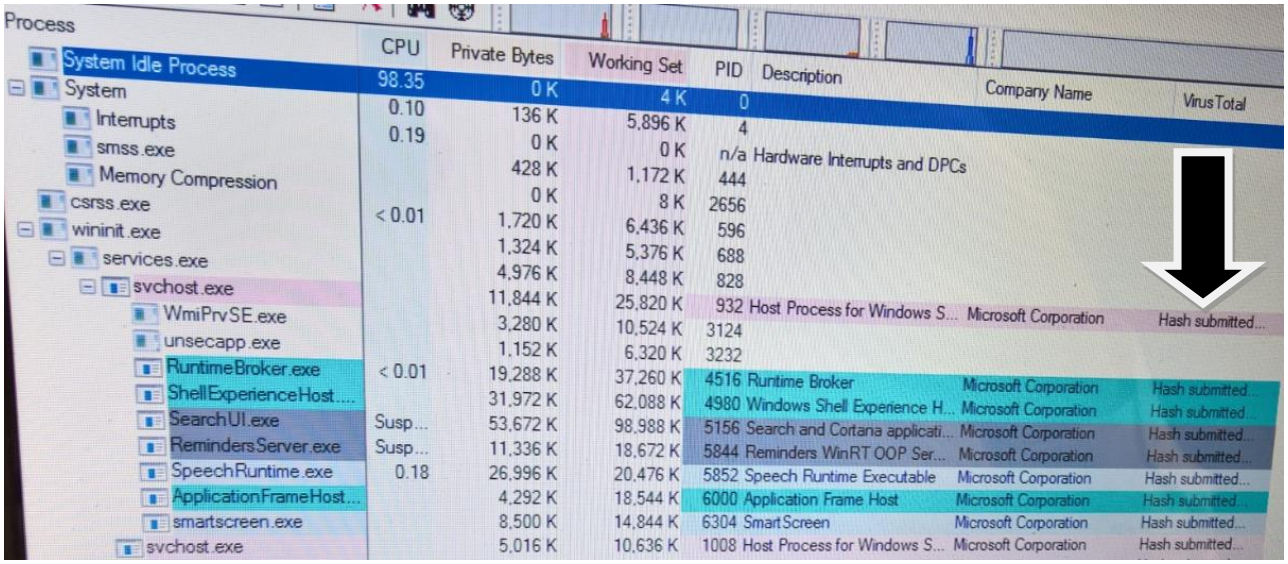
I right-clicked on the icon for the larger application file and got the following window where I clicked on Pin to taskbar. That action put the Process Explorer icon in the taskbar.



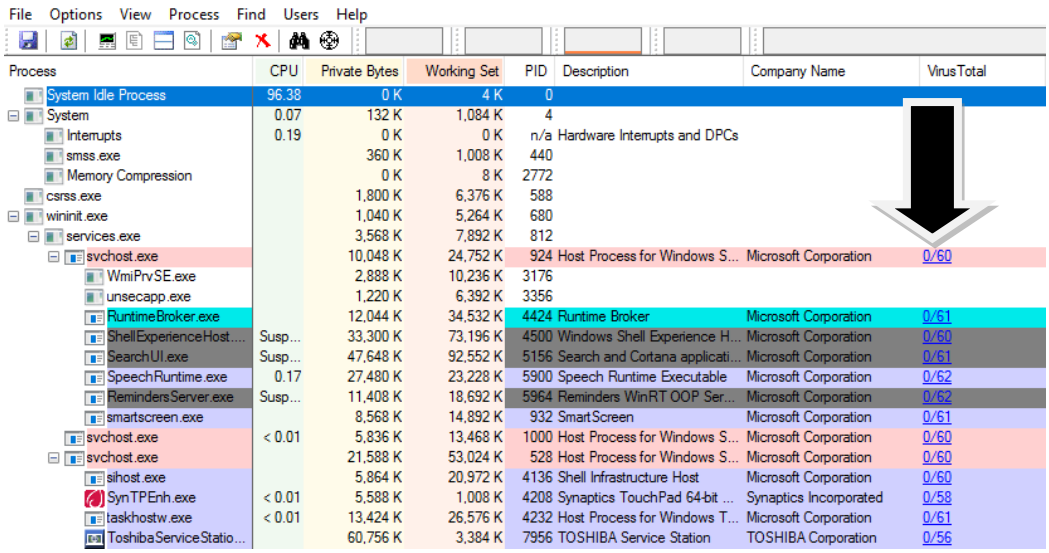
When to use

As mentioned earlier, whenever I suspect a problem on my computer that may be associated with malware, I left-click on the Process Explorer icon on the taskbar.

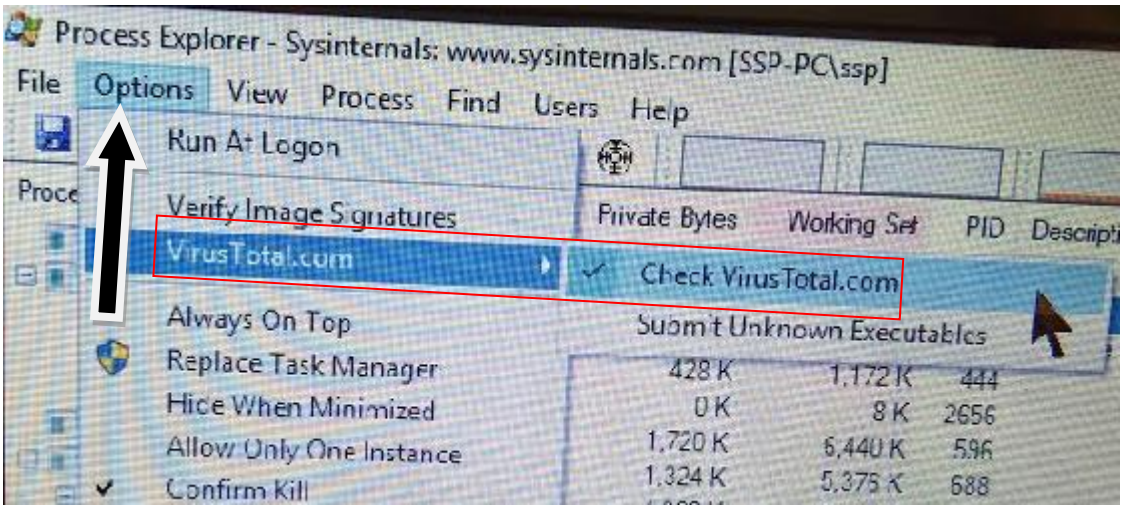
That action should result in the following partial display. (If not, see next page) The arrow points to the notation that hash code has been submitted.



As shown by the arrow below, after a short period following when the code "snapshot" is sent to a number of reviewers, those reviewers respond and their results are tabulated. When malicious code is reported, the number of reviewers reporting malicious code is shown in red. In this example below, no malicious code was found.



If after left-clicking on the Process Explorer icon on the taskbar as described earlier, the display does not show that hash code has been submitted, left-click on the Options link as shown by the arrow below, then left-click on VirusTotal.com and Check VirusTotal.com in the box as shown by the red outline. That should produce the screens shown earlier.



How to use

If a significant number of reviewers report malicious code, click on the red link(s) and follow any instructions provided by the program. Other security programs such as Malwarebytes and Windows Defender or Security Essentials should also be run. If no malicious code is reported, close Process Explorer and continue what you were doing.