

Title: Installation and Demonstration of System Internal Tool (Process Explorer) for Data Classification by Process ID and Company Name

Objective:

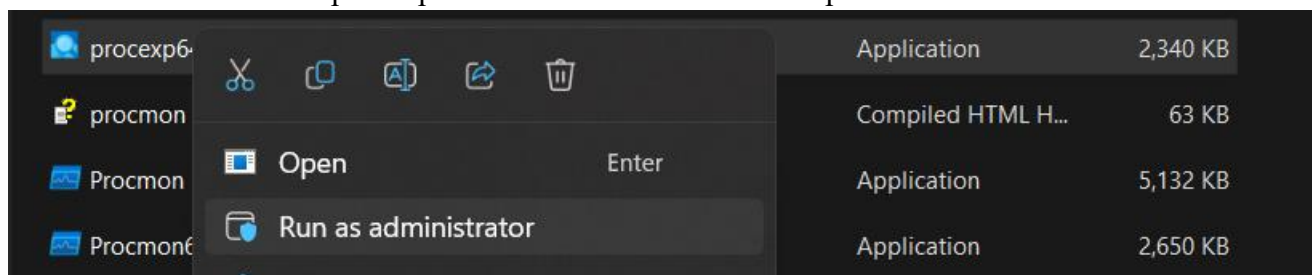
The objective of this experiment is to install and demonstrate the usage of the System Internal Tool called Process Explorer. Additionally, we aim to classify data using process ID and company name information obtained from Process Explorer.

Requirements:

Sysinternal suite

Procedure/Experiment Steps:

1. Download Process Explorer:
 - a. Open a web browser.
 - b. Visit the official Microsoft website.
 - c. Search for "Process Explorer" or Sysinternal suite and navigate to the official download page.
 - d. Download the appropriate version that compatible with your Windows operating system.
 - e. Save the downloaded file.
2. Launch Process Explorer:
 - a. Navigate to the installation location of Process Explorer.
 - b. Double-click on the "procxp.exe" file to launch Process Explorer.



- c. It will ask for the installation for the first time only.
3. Explore Process Explorer Interface:
 - a. The Process Explorer interface, which provides a comprehensive view of running processes on your system.
 - b. Observe the various columns displayed, including process name, process ID, company name, CPU usage, memory usage, etc.

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
Secure System	Susp...	30,828 K	108			
Registry		9,064 K	56,728 K	144		
System Idle Process	97.08	60 K	8 K	0		
System	0.37	60 K	124 K	4		
Interrupts	0.18	0 K	0 K	n/a	Hardware Interrupts and DPCs	
smss.exe		1,116 K	1,048 K	556		
Memory Compression	< 0.01	1,396 K	1,03,632 K	4152		
csrss.exe		2,344 K	5,448 K	1004		
wininit.exe		1,604 K	5,728 K	936		
services.exe	< 0.01	6,396 K	10,000 K	1008		
svchost.exe	< 0.01	19,264 K	68,824 K	1248	Host Process for Windows S...	Microsoft Corporation
WmiPrvSE.exe		11,284 K	23,352 K	5216	WMI Provider Host	Microsoft Corporation
unsecapp.exe		1,976 K	7,660 K	5520	Sink to receive asynchronous...	Microsoft Corporation
SearchHost.exe	Susp...	1,90,004 K	1,19,528 K	10620		Microsoft Corporation
StartMenuExperienceHo...		51,964 K	86,308 K	10564	Windows Start Experience H...	Microsoft Corporation
Widgets.exe		8,176 K	36,636 K	20996		Microsoft Corporation
RuntimeBroker.exe		6,612 K	23,096 K	15648	Runtime Broker	Microsoft Corporation
RuntimeBroker.exe		16,520 K	54,424 K	10164	Runtime Broker	Microsoft Corporation
dllhost.exe		6,340 K	15,972 K	13968	COM Surrogate	Microsoft Corporation
WidgetService.exe		4,620 K	22,728 K	7448		
TextInputHost.exe	< 0.01	3,60,980 K	3,69,528 K	20888		Microsoft Corporation
ShellExperienceHost.exe	Susp...	35,656 K	65,424 K	11172	Windows Shell Experience H...	Microsoft Corporation
RuntimeBroker.exe		3,660 K	18,360 K	16572	Runtime Broker	Microsoft Corporation
unsecapp.exe		1,680 K	8,900 K	13884	Sink to receive asynchronous...	Microsoft Corporation
SpeechWidgetProvider.e...		10,816 K	29,372 K	17196		
AcrobatNotificationClient...	Susp...	15,516 K	4,560 K	4776		
RuntimeBroker.exe		1,304 K	7,616 K	18792	Runtime Broker	Microsoft Corporation
SystemSettings.exe	Susp...	59,920 K	3,952 K	15344	Settings	Microsoft Corporation
ApplicationFrameHost.e...		17,980 K	39,520 K	13868	Application Frame Host	Microsoft Corporation
UserOOBEBroker.exe		2,100 K	9,796 K	17680	User OOBEBroker	Microsoft Corporation
SDXHelper.exe	< 0.01	11,512 K	22,984 K	16636	Microsoft Office SDX Helper	Microsoft Corporation
WhatsApp.exe	< 0.01	1,40,516 K	2,01,604 K	20056		
RuntimeBroker.exe		8,972 K	32,868 K	7488	Runtime Broker	Microsoft Corporation
dllhost.exe		1,420 K	9,560 K	20296	COM Surrogate	Microsoft Corporation
SmartScreen.exe		5,066 K	21,120 K	15012	Windows Defender SmartScr...	Microsoft Corporation
WmiPrvSE.exe		3,924 K	11,756 K	18260	WMI Provider Host	Microsoft Corporation
WUDFHost.exe		14,688 K	24,536 K	1292	Windows Driver Foundation -	Microsoft Corporation
svchost.exe	< 0.01	13,812 K	25,200 K	1424	Host Process for Windows S...	Microsoft Corporation
svchost.exe		3,868 K	10,388 K	1476	Host Process for Windows S...	Microsoft Corporation
svchost.exe		1,728 K	5,252 K	1652	Host Process for Windows S...	Microsoft Corporation
svchost.exe		3,460 K	8,648 K	1660	Host Process for Windows S...	Microsoft Corporation
svchost.exe	< 0.01	8,128 K	11,232 K	1684	Host Process for Windows S...	Microsoft Corporation
svchost.exe		3,928 K	14,784 K	1804	Host Process for Windows S...	Microsoft Corporation
svchost.exe		7,608 K	15,404 K	1820	Host Process for Windows S...	Microsoft Corporation
DropboxUpdate.exe		2,176 K	10,716 K	2518	Dropbox Update	Dropbox, Inc.
taskhostw.exe		9,884 K	21,916 K	6264	Host Process for Windows T...	Microsoft Corporation
SystemOptimizer.exe	< 0.01	43,580 K	25,276 K	16872	HP OMEN SystemOptimizer	HP Inc.

CPU Usage: 3.51% | Commit Charge: 58.48% | Physical Usage: 77.21%

4. Data Classification by Process ID:

- Identify the process ID (PID) column in Process Explorer.

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
Interrupts	0.19	0 K	0 K	n/a	Hardware Interrupts and DPCs	
System Idle Process	94.74	60 K	8 K	0		
System	0.37	60 K	124 K	4		
Secure System	Susp...	188 K	30,828 K	108		
...		19,476 K	58,968 K	144		

- Analyse the PID values associated with different processes.
- Classify or categorize the data based on the process IDs. For example, you can group processes by their PID ranges or assign specific actions based on PID values.

5. Data Classification by Company Name:

- Identify the company name column in Process Explorer.

Company Name
Adobe Systems Incorporated
Microsoft Corporation
Microsoft Corporation
HP Inc.
Microsoft Corporation
Adobe Inc.
Microsoft Corporation
Microsoft Corporation
Microsoft Corporation
BraveSoftware Inc.
BraveSoftware Inc.
Microsoft Corporation
Microsoft Corporation
Microsoft Corporation

- Analyse the company names associated with different processes.
- Classify or categorize the data based on the company names. For example, you can group processes by the company name or apply specific policies based on the company's reputation.

Result:

The obtained results from Process Explorer allow for efficient data classification based on process ID and company name. By grouping processes using process ID or company name, you can gain insights into system activity and make informed decisions regarding resource allocation, security policies, and more.

Conclusion:

In conclusion process Explorer is a powerful tool for monitoring and managing processes on a Windows system. The ability to classify data based on process ID and company name and other parameter enhances process analysis and decision-making capabilities, contributing to improved system performance and security.

Future Scope:

1. Further research and experimentation can explore additional criteria for data classification, such as process hierarchy, resource utilization, or network activity.
2. Integration of Process Explorer data with other security tools or automation scripts can enhance system monitoring and incident response capabilities.
3. Investigating process anomalies or suspicious behaviour abased on process ID and company name can lead to the development of advanced threat detection techniques.
4. Continual updates and enhancements to Process Explorer by Microsoft may introduce new features and functionalities for data classification and analysis.