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.

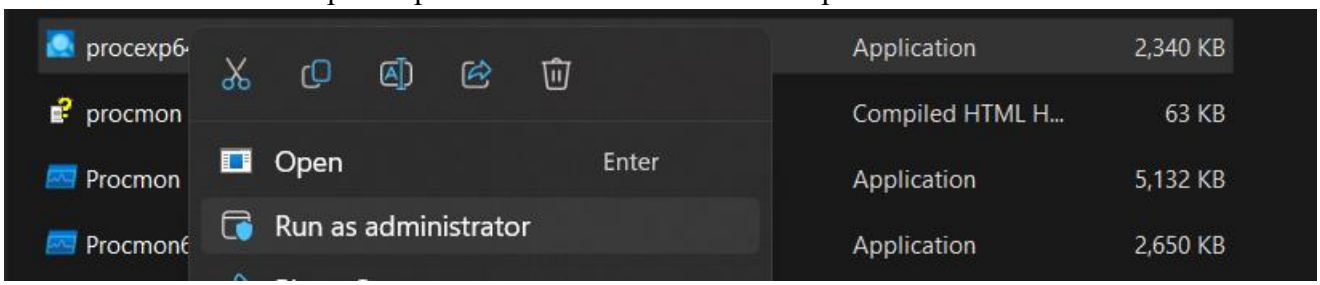
Requirements:

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.

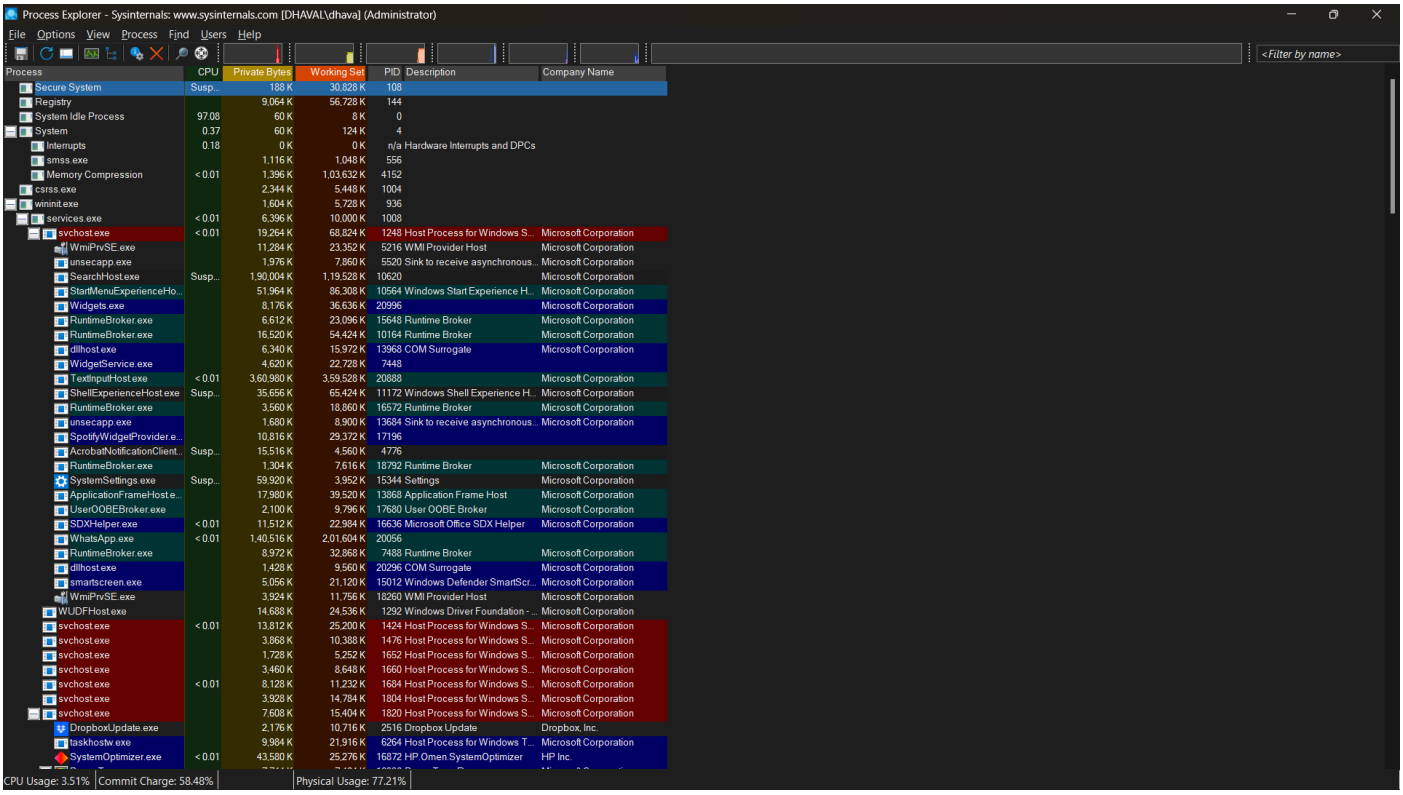
2. Launch Process Explorer:
    a. Navigate to the installation location of Process Explorer.
    b. Double-click on the "procexp.exe" file to launch Process Explorer.



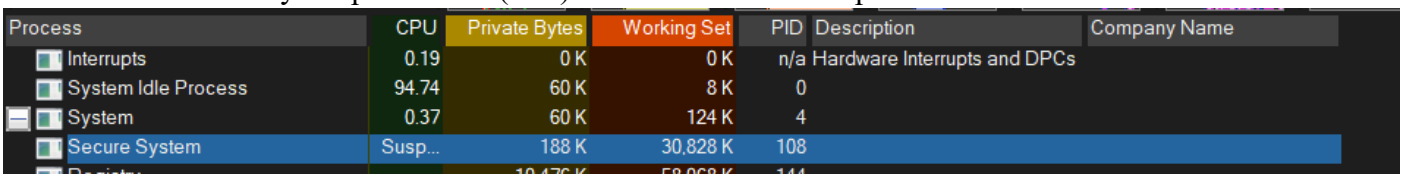
    c. It will ask for the installation for the first time only.

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.



4. Data Classification by Process ID:
    a. Identify the process ID (PID) column in Process Explorer.



    b. Analyse the PID values associated with different processes.
    c. 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:
    a. Identify the company name column in Process Explorer.

    b. Analyse the company names associated with different processes.
    c. 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 perameter 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.