Process Explorer

By: Mohammad Basmalah

1. Proses explorer

Process Explorer adalah program komputer freeware untuk Microsoft Windows diciptakan oleh Sysinternals, yang telah diakuisisi oleh Microsoft Corporation.
Process Explorer adalah sistem pemantauan dan utilitas pemeriksaan. Ini menyediakan fungsionalitas Windows Task Manager bersama dengan satu set kaya fitur untuk mengumpulkan informasi tentang proses yang berjalan pada sistem pengguna. Hal ini dapat digunakan sebagai langkah pertama dalam debugging perangkat lunak atau sistem masalah.

Process Explorer dapat digunakan untuk melacak masalah. Misalnya, menyediakan sarana untuk daftar atau mencari sumber daya bernama yang dimiliki oleh sebuah proses atau semua proses. Ini dapat digunakan untuk melacak apa yang memegang file yang terbuka dan mencegah penggunaannya oleh program lain. Atau sebagai contoh lain, dapat menunjukkan garis perintah digunakan untuk memulai sebuah program, yang memungkinkan proses dinyatakan identik harus dibedakan. Atau seperti Task Manager, dapat menunjukkan sebuah proses yang maxing CPU, tapi tidak seperti Task Manager dapat menunjukkan mana thread (dengan callstack) menggunakan CPU – informasi yang bahkan tidak tersedia di bawah debugger.

2. Fitur-Fitur Process Explorer

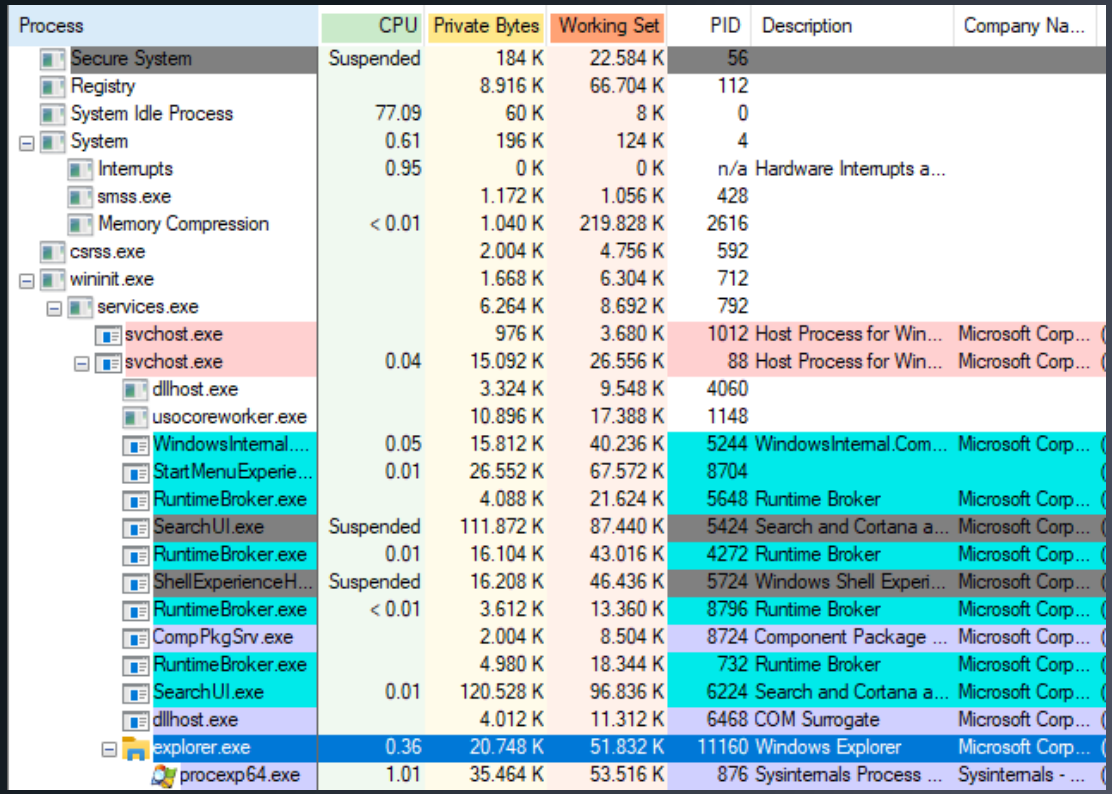
A. Process Tree Pada Process Explorer

B. Memahami Warna Yang Terdapat Pada Process Explorer

C. Tindakan Yang Dapat Dilakukan Process Explorer

A. Process Tree Pada Process Explorer

Adalah keseluruhan tampilan process yang bekerja pada komputer kita dengan menampilkannya secara hirarki. Biasanya akan langsung muncul pada saat kita mambuka aplikasi process explorer



Process	CPU	Private Bytes	Working Set	PID	Description	Company Na...
Secure System	Suspended	184 K	22.584 K	56		
Registry		8.916 K	66.704 K	112		
System Idle Process	77.09	60 K	8 K	0		
System	0.61	196 K	124 K	4		
Interrupts	0.95	0 K	0 K	n/a	Hardware Interrupts a...	
smss.exe		1.172 K	1.056 K	428		
Memory Compression	< 0.01	1.040 K	219.828 K	2616		
csrss.exe		2.004 K	4.756 K	592		
wininit.exe		1.668 K	6.304 K	712		
services.exe		6.264 K	8.692 K	792		
svchost.exe		976 K	3.680 K	1012	Host Process for Win...	Microsoft Corp...
svchost.exe	0.04	15.092 K	26.556 K	88	Host Process for Win...	Microsoft Corp...
dllhost.exe		3.324 K	9.548 K	4060		
usocoreworker.exe		10.896 K	17.388 K	1148		
WindowsInternal....	0.05	15.812 K	40.236 K	5244	WindowsInternal.Com...	Microsoft Corp...
StartMenuExperie...	0.01	26.552 K	67.572 K	8704		
RuntimeBroker.exe		4.088 K	21.624 K	5648	Runtime Broker	Microsoft Corp...
SearchUI.exe	Suspended	111.872 K	87.440 K	5424	Search and Cortana a...	Microsoft Corp...
RuntimeBroker.exe	0.01	16.104 K	43.016 K	4272	Runtime Broker	Microsoft Corp...
ShellExperienceH...	Suspended	16.208 K	46.436 K	5724	Windows Shell Experi...	Microsoft Corp...
RuntimeBroker.exe	< 0.01	3.612 K	13.360 K	8796	Runtime Broker	Microsoft Corp...
CompPkgSrv.exe		2.004 K	8.504 K	8724	Component Package ...	Microsoft Corp...
RuntimeBroker.exe		4.980 K	18.344 K	732	Runtime Broker	Microsoft Corp...
SearchUI.exe	0.01	120.528 K	96.836 K	6224	Search and Cortana a...	Microsoft Corp...
dllhost.exe		4.012 K	11.312 K	6468	COM Surrogate	Microsoft Corp...
explorer.exe	0.36	20.748 K	51.832 K	11160	Windows Explorer	Microsoft Corp...
procexp64.exe	1.01	35.464 K	53.516 K	876	Sysinternals Process ...	Sysinternals - ...

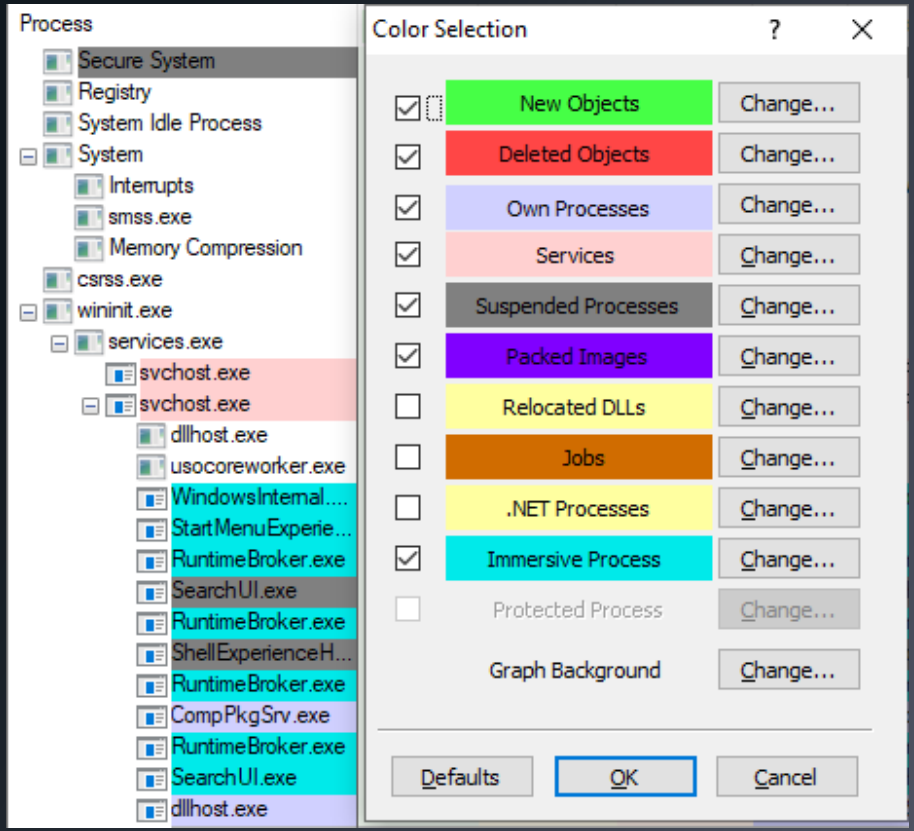
Tampilan awal yang ada di process explorer

- Proses: nama file yang berjalan serta ikonnya
- CPU: persentase waktu CPU di detik akhir
- Private Bytes: jumlah memory yang dialokasikan untuk satu program saja
- Working Set: jumlah RAM aktual yang dialokasi untuk satu program
- PID: Pengidentifikasi proses
- Description: Deskripsi (jika aplikasi memilikinya)
- Company Name: nama perusahaan dari sebuah aplikasi

Biasanya tampilan akan diperbaharui sekali tiap detik, atau dapat diatur sesuai kengininan dengan cara klik view – update speed (batas minimum 0.5s sampai 10s). Kita juga dapat memberhentikan sementara tampilan dengan menggunakan spasi pada keyboard

B. Memahami Warna Yang Terdapat Pada Process Explorer

Terdapat beberapa warna didalam program Process Explorer. Warna-warna tersebut memiliki arti tersendiri bagi setiap process yang terdaftar pada Process Explorer. Sangat penting untuk kita mengetahui mempelajari atau mengetahui warna-warna tersebut

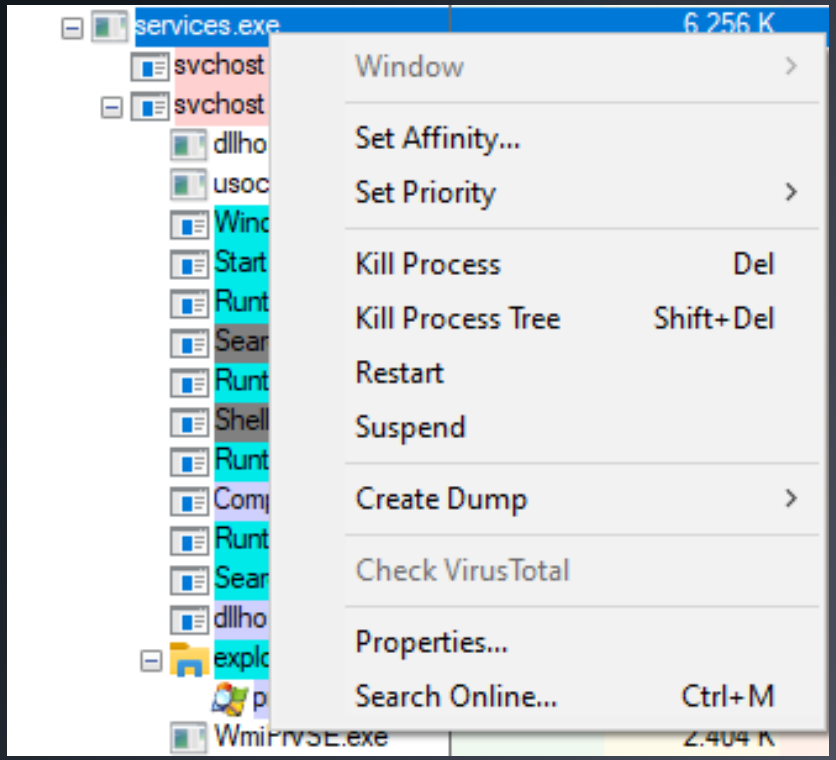


- Hijau cerah (New Object), ketika proses baru muncul di proses explorer, maka proses tersebut akan berwarna hijau cerah
- Merah (Deleted Object), jika kita menutup suatu program, maka pada tampilan proses akan muncul warna merah terlebih dahulu sebelum menghilang/terhapus
- Lavender Biru (Owner Process), proses yang berjalan sebagai akun pengguna yang sama dengan proses explorer.
- Pink Cerah (Service), Proses Windows Service, meskipun perlu dicatat bahwa mereka mungkin memiliki proses turunan yang diluncurkan sebagai pengguna yang berbeda, dan itu mungkin warna yang berbeda.
- Abu-Abu Gelap (suspended Process), proses yang ditangguhkan atau diberhentikan
- Ungu (Packed Images), proses ini mungkin berisi kode terkompresi yang tersembunyi di dalamnya, atau setidaknya Process Explorer berpikir bahwa mereka melakukannya dengan menggunakan heuristik. Jika Anda melihat proses berwarna ungu, pastikan untuk memindai malware
- Biru terang (Immersive Process), Ini hanyalah cara mewah untuk mengatakan bahwa prosesnya adalah aplikasi Windows 8 menggunakan API baru

Kita juga dapat merubah warna-warna tersebut sesuai keinginan kita, dengan cara klik *Options* lalu pilih *configure color*.

C. Tindakan Yang Dapat Dilakukan Process Explorer

Ada beberapa tindakan yang dapat kita lakukan di dalam process Explorer tersebut. Diantaranya kita dapat membunuh suatu proses, memuat ulang proses, menghentikan proses, dll.



- Window, memiliki opsi termasuk Bawa ke Depan, yang dapat berguna untuk membantu mengidentifikasi jendela yang terkait dengan suatu proses. Jika tidak ada jendela untuk proses itu, maka akan berwarna abu-abu
- Set Priority, jika kita ingin mengatur sebuah proses menjadi priortas kita dapat memilih set priority
- Kill Proses, membunuh atau menghentikan sebuah proses
- Kill Process Tree, seperti kill proses tetapi akan membunuh semua proses yang berkaitan dengan proses induk nya
- Restart, mengulang kembali sebuah proses
- Suspend, menghentikan sementara sebuah proses
- Check VirusTotal, Ini sangat berguna, karena ia memeriksa proses untuk virus
- Search Online, ini hanya akan mencari web untuk nama prosesnya

Thank You