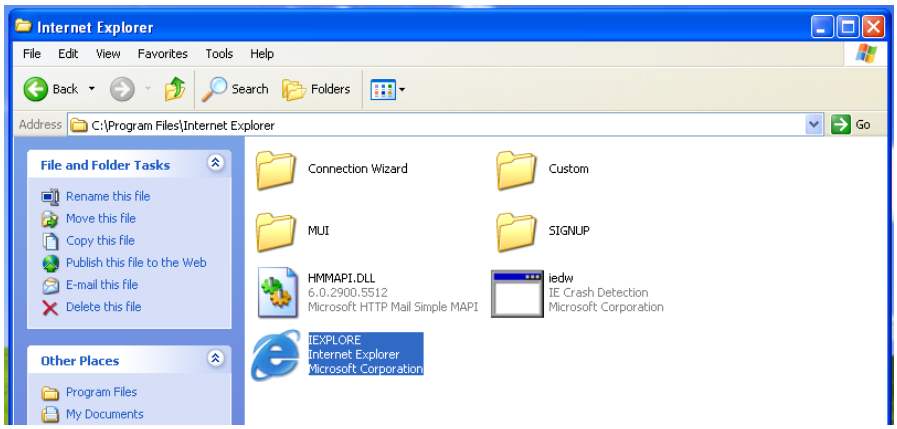
Un giovane dipendente neo assunto segnala al reparto tecnico la presenza di un programma sospetto.

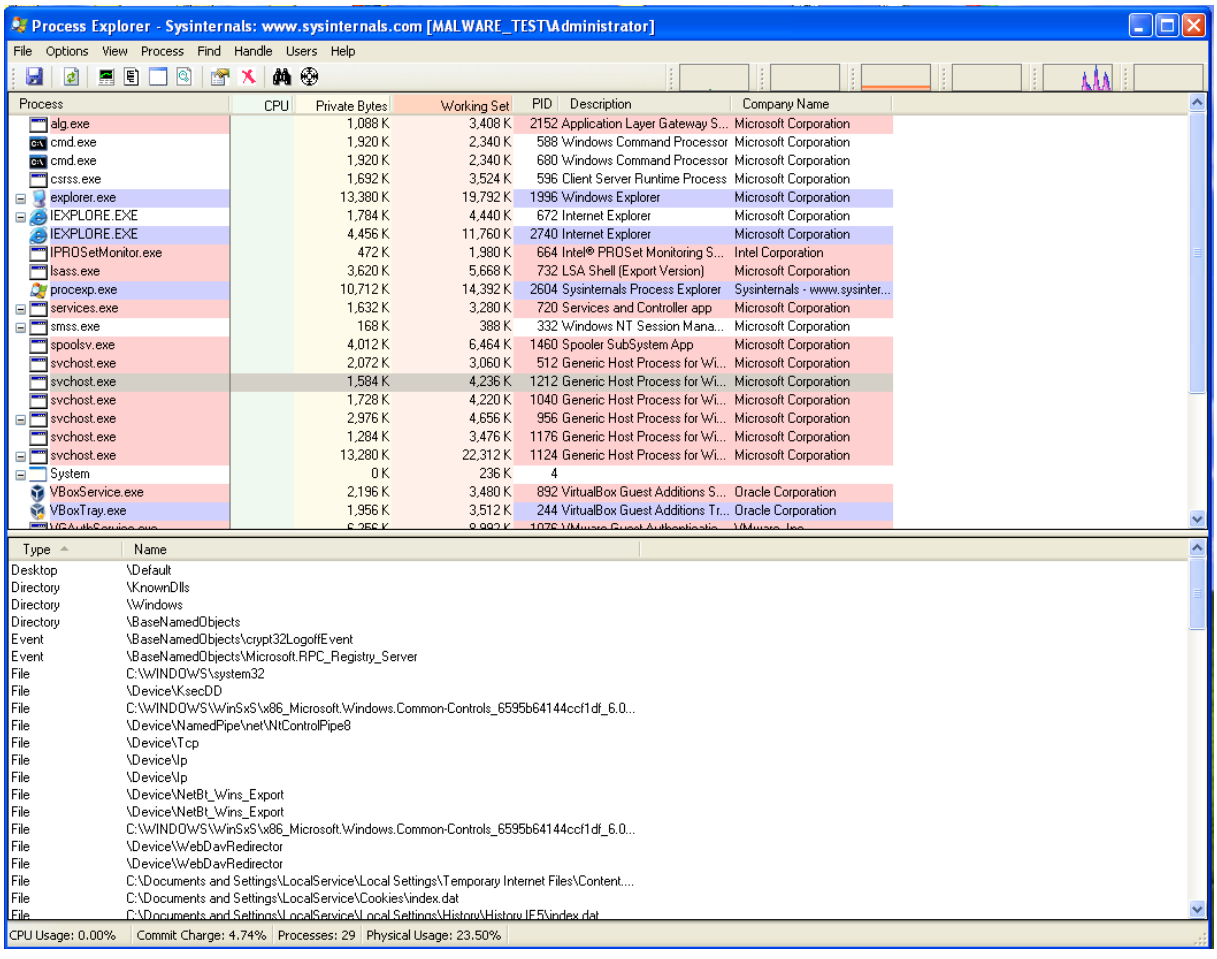
Il suo superiore gli dice di stare tranquillo ma lui non è soddisfatto e chiede supporto al SOC. Il file "sospetto" è IEXPLORE.EXE contenuto nella cartella C:\Program Files\Internet Explorer

E' richiesto di convincere il dipendente che il file non è maligno.

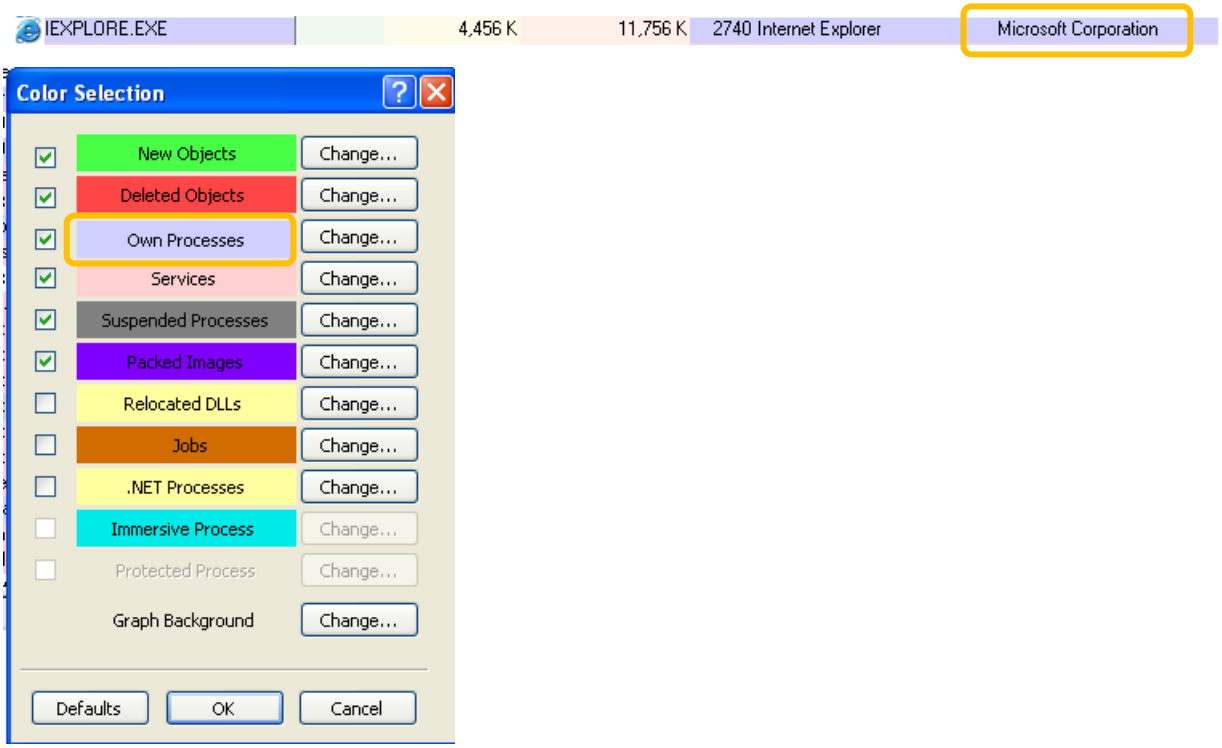
Avviamo `IEXPLORE.EXE`



Avviamo Process Explorer

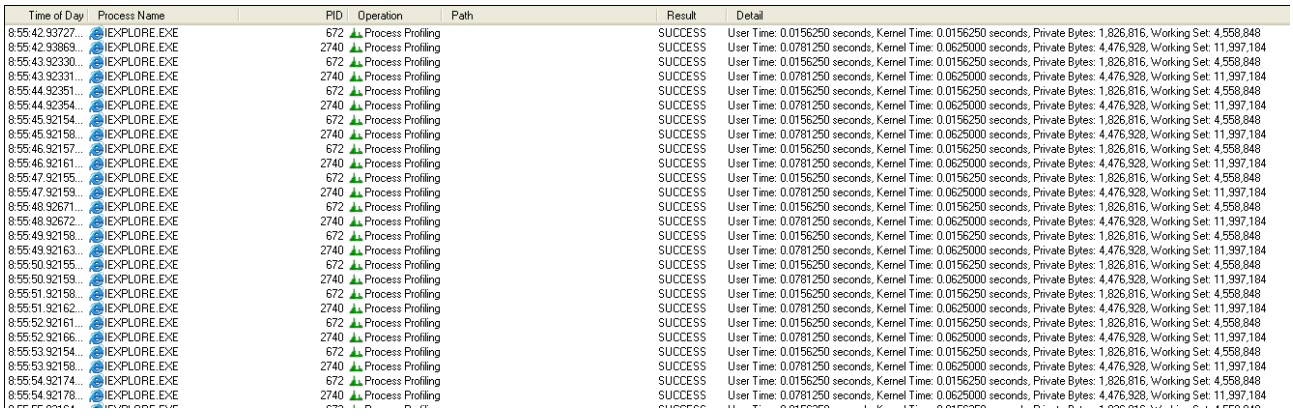


Vediamo che `IEXPLORE.EXE` è colorato di lilla. Nelle impostazioni dei colori questo indica che si tratta di un processo di sistema. La colonna Company Name, inoltre riporta “Microsoft Corporation”.



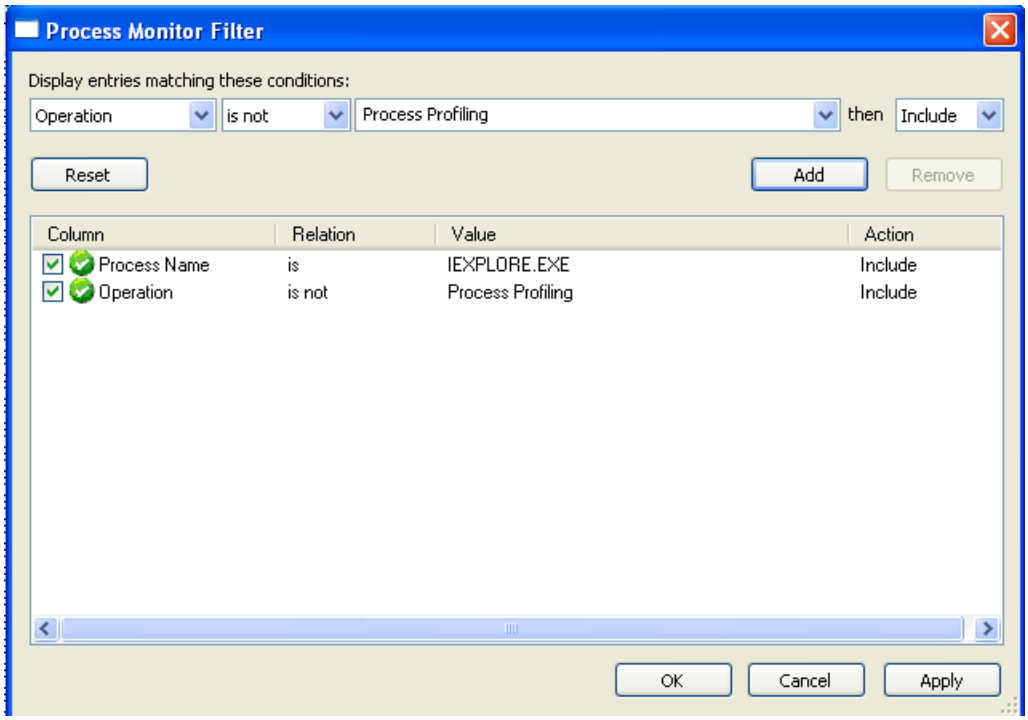
Apriamo ora Process Monitor e filtriamo il processo `IEXPLORE.EXE`. Notiamo esclusivamente l’operazione **`PocessProfiling`.**

Si tratta di un’attività specifica di Process Monitor, che ha la capacità di intercettare una vasta gamma di eventi del sistema, comprese le chiamate di profiling. Nello specifico, questa operazione riguarda la raccolta di statistiche sulle prestazioni del processo.

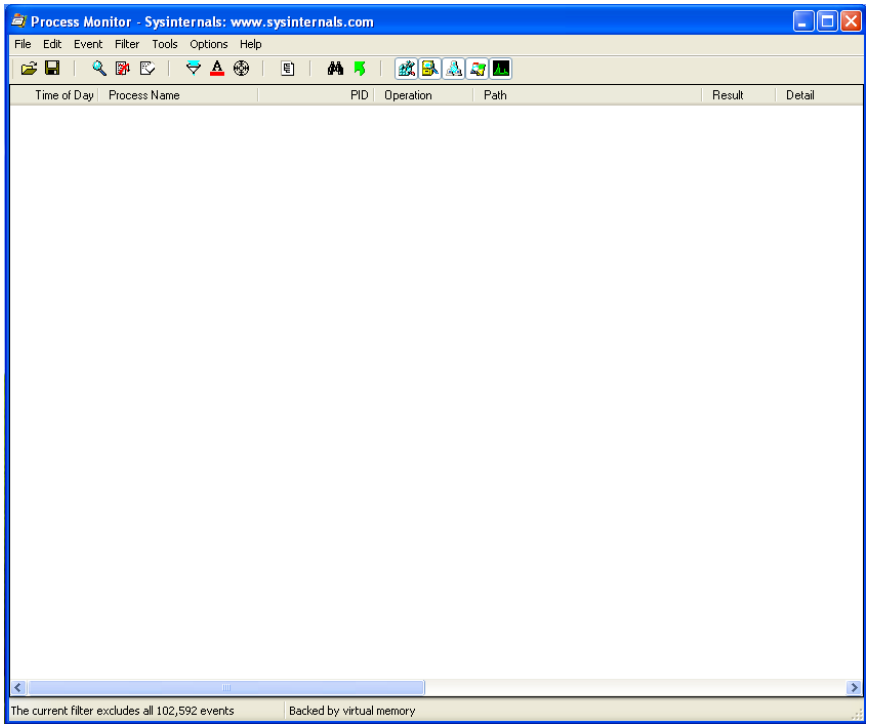


Time of Day	Process Name	PID	Operation	Path	Result	Detail
8:55:42.93727...	IEXPLORE.EXE	672	Process Profiling		SUCCESS	User Time: 0.0156250 seconds, Kernel Time: 0.0156250 seconds, Private Bytes: 1,826,816, Working Set: 4,558,848
8:55:42.93869...	IEXPLORE.EXE	2740	Process Profiling		SUCCESS	User Time: 0.0781250 seconds, Kernel Time: 0.0625000 seconds, Private Bytes: 4,476,928, Working Set: 11,997,184
8:55:43.92330...	IEXPLORE.EXE	672	Process Profiling		SUCCESS	User Time: 0.0156250 seconds, Kernel Time: 0.0156250 seconds, Private Bytes: 1,826,816, Working Set: 4,558,848
8:55:43.92331...	IEXPLORE.EXE	2740	Process Profiling		SUCCESS	User Time: 0.0781250 seconds, Kernel Time: 0.0625000 seconds, Private Bytes: 4,476,928, Working Set: 11,997,184
8:55:44.92351...	IEXPLORE.EXE	672	Process Profiling		SUCCESS	User Time: 0.0156250 seconds, Kernel Time: 0.0156250 seconds, Private Bytes: 1,826,816, Working Set: 4,558,848
8:55:44.92354...	IEXPLORE.EXE	2740	Process Profiling		SUCCESS	User Time: 0.0781250 seconds, Kernel Time: 0.0625000 seconds, Private Bytes: 4,476,928, Working Set: 11,997,184
8:55:45.92154...	IEXPLORE.EXE	672	Process Profiling		SUCCESS	User Time: 0.0156250 seconds, Kernel Time: 0.0156250 seconds, Private Bytes: 1,826,816, Working Set: 4,558,848
8:55:45.92158...	IEXPLORE.EXE	2740	Process Profiling		SUCCESS	User Time: 0.0781250 seconds, Kernel Time: 0.0625000 seconds, Private Bytes: 4,476,928, Working Set: 11,997,184
8:55:46.92157...	IEXPLORE.EXE	672	Process Profiling		SUCCESS	User Time: 0.0156250 seconds, Kernel Time: 0.0156250 seconds, Private Bytes: 1,826,816, Working Set: 4,558,848
8:55:46.92161...	IEXPLORE.EXE	2740	Process Profiling		SUCCESS	User Time: 0.0781250 seconds, Kernel Time: 0.0625000 seconds, Private Bytes: 4,476,928, Working Set: 11,997,184
8:55:47.92155...	IEXPLORE.EXE	672	Process Profiling		SUCCESS	User Time: 0.0156250 seconds, Kernel Time: 0.0156250 seconds, Private Bytes: 1,826,816, Working Set: 4,558,848
8:55:47.92159...	IEXPLORE.EXE	2740	Process Profiling		SUCCESS	User Time: 0.0781250 seconds, Kernel Time: 0.0625000 seconds, Private Bytes: 4,476,928, Working Set: 11,997,184
8:55:48.92671...	IEXPLORE.EXE	672	Process Profiling		SUCCESS	User Time: 0.0156250 seconds, Kernel Time: 0.0156250 seconds, Private Bytes: 1,826,816, Working Set: 4,558,848
8:55:48.92672...	IEXPLORE.EXE	2740	Process Profiling		SUCCESS	User Time: 0.0781250 seconds, Kernel Time: 0.0625000 seconds, Private Bytes: 4,476,928, Working Set: 11,997,184
8:55:49.92158...	IEXPLORE.EXE	672	Process Profiling		SUCCESS	User Time: 0.0156250 seconds, Kernel Time: 0.0156250 seconds, Private Bytes: 1,826,816, Working Set: 4,558,848
8:55:49.92163...	IEXPLORE.EXE	2740	Process Profiling		SUCCESS	User Time: 0.0781250 seconds, Kernel Time: 0.0625000 seconds, Private Bytes: 4,476,928, Working Set: 11,997,184
8:55:50.92155...	IEXPLORE.EXE	672	Process Profiling		SUCCESS	User Time: 0.0156250 seconds, Kernel Time: 0.0156250 seconds, Private Bytes: 1,826,816, Working Set: 4,558,848
8:55:50.92159...	IEXPLORE.EXE	2740	Process Profiling		SUCCESS	User Time: 0.0781250 seconds, Kernel Time: 0.0625000 seconds, Private Bytes: 4,476,928, Working Set: 11,997,184
8:55:51.92158...	IEXPLORE.EXE	672	Process Profiling		SUCCESS	User Time: 0.0156250 seconds, Kernel Time: 0.0156250 seconds, Private Bytes: 1,826,816, Working Set: 4,558,848
8:55:51.92162...	IEXPLORE.EXE	2740	Process Profiling		SUCCESS	User Time: 0.0781250 seconds, Kernel Time: 0.0625000 seconds, Private Bytes: 4,476,928, Working Set: 11,997,184
8:55:52.92161...	IEXPLORE.EXE	672	Process Profiling		SUCCESS	User Time: 0.0156250 seconds, Kernel Time: 0.0156250 seconds, Private Bytes: 1,826,816, Working Set: 4,558,848
8:55:52.92166...	IEXPLORE.EXE	2740	Process Profiling		SUCCESS	User Time: 0.0781250 seconds, Kernel Time: 0.0625000 seconds, Private Bytes: 4,476,928, Working Set: 11,997,184
8:55:53.92154...	IEXPLORE.EXE	672	Process Profiling		SUCCESS	User Time: 0.0156250 seconds, Kernel Time: 0.0156250 seconds, Private Bytes: 1,826,816, Working Set: 4,558,848
8:55:53.92158...	IEXPLORE.EXE	2740	Process Profiling		SUCCESS	User Time: 0.0781250 seconds, Kernel Time: 0.0625000 seconds, Private Bytes: 4,476,928, Working Set: 11,997,184
8:55:54.92174...	IEXPLORE.EXE	672	Process Profiling		SUCCESS	User Time: 0.0156250 seconds, Kernel Time: 0.0156250 seconds, Private Bytes: 1,826,816, Working Set: 4,558,848
8:55:54.92178...	IEXPLORE.EXE	2740	Process Profiling		SUCCESS	User Time: 0.0781250 seconds, Kernel Time: 0.0625000 seconds, Private Bytes: 4,476,928, Working Set: 11,997,184

Oltre al filtro sul processo `IEXPLORE.EXE`, applichiamo su Process Monitor un filtro che esclude Operazioni di tipo `ProcessProfiling`, che abbiamo visto sono operazioni innocue.



Applicando il filtro, vediamo che Process Monitor non ha registrato altre operazioni legate al processo `IEXPLORE.EXE`.



Questo esclude l'eventualità che il processo `IEXPLORE.EXE` possa essere in qualche modo dannoso per il sistema.