Tutorials

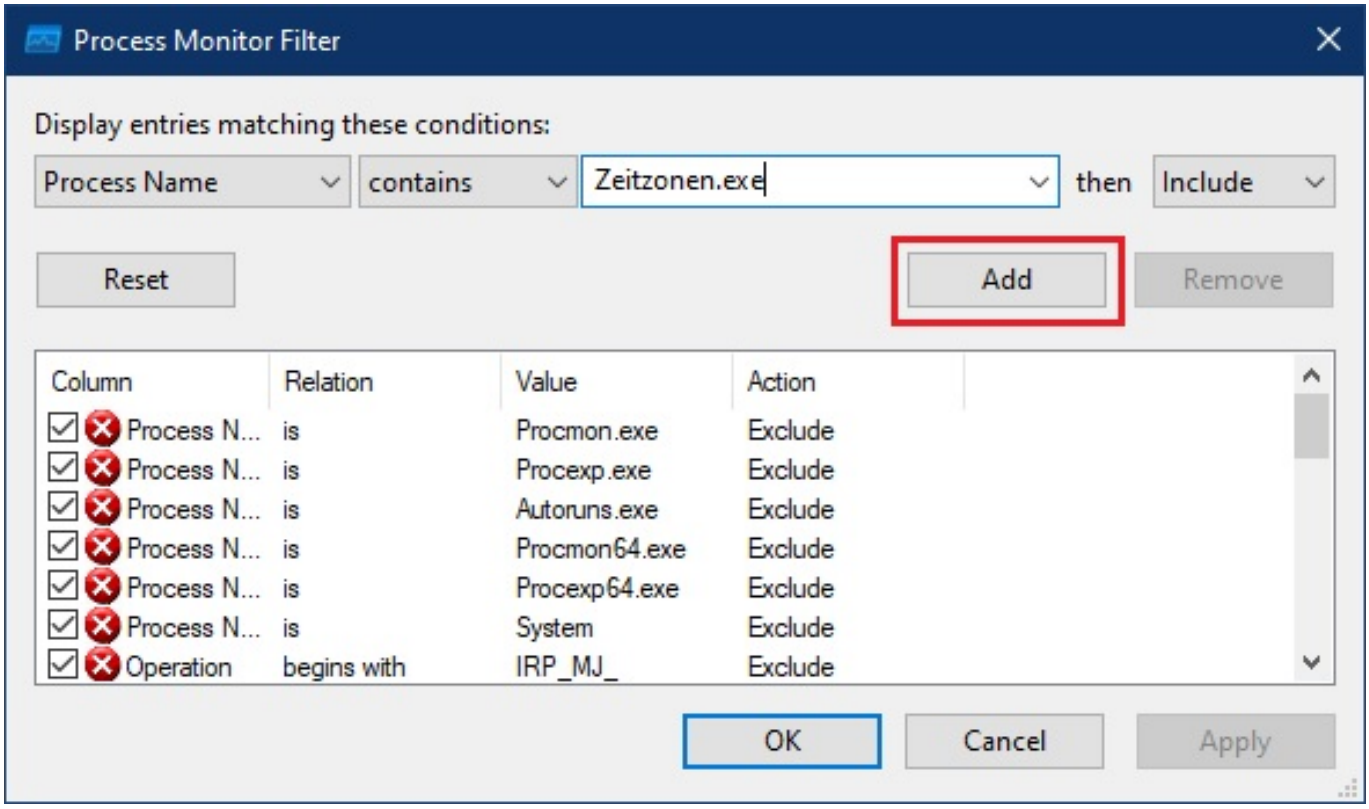
Tutorial (deutsch): Wie kann ich mit dem Process Monitor von Windows Sysinternals einen Prozess in Windows überwachen?

- Mit dem kostenlosen Analyse-Tool **Process Monitor**, welches Sie auch auf der Webseite von **Microsoft** erhalten, können Sie sämtliche auf Ihrem Rechner bzw. PC ausgeführten **System-Prozesse** überwachen.
- So sehen Sie z.B., wenn ein Programm auf einen anderen IP-Bereich zugreift, wann es aus der **Registry** liest bzw. in die Registry schreibt etc.
- Wenn Sie sich den **Process Monitor** heruntergeladen haben, starten Sie diesen über die Datei Procmon.exe (Sie müssen anschließend in Windows bestätigen, dass durch diese App Änderungen an ihrem Gerät vorgenommen werden).
- Wurde das Programm gestartet, beginnt es direkt mit der Aufzeichnung der **Systemprozesse**.
- Sie können die **Aufzeichnung** über einen Klick auf das Capture-Icon oder über die Tastenkombination Strg + E beenden.

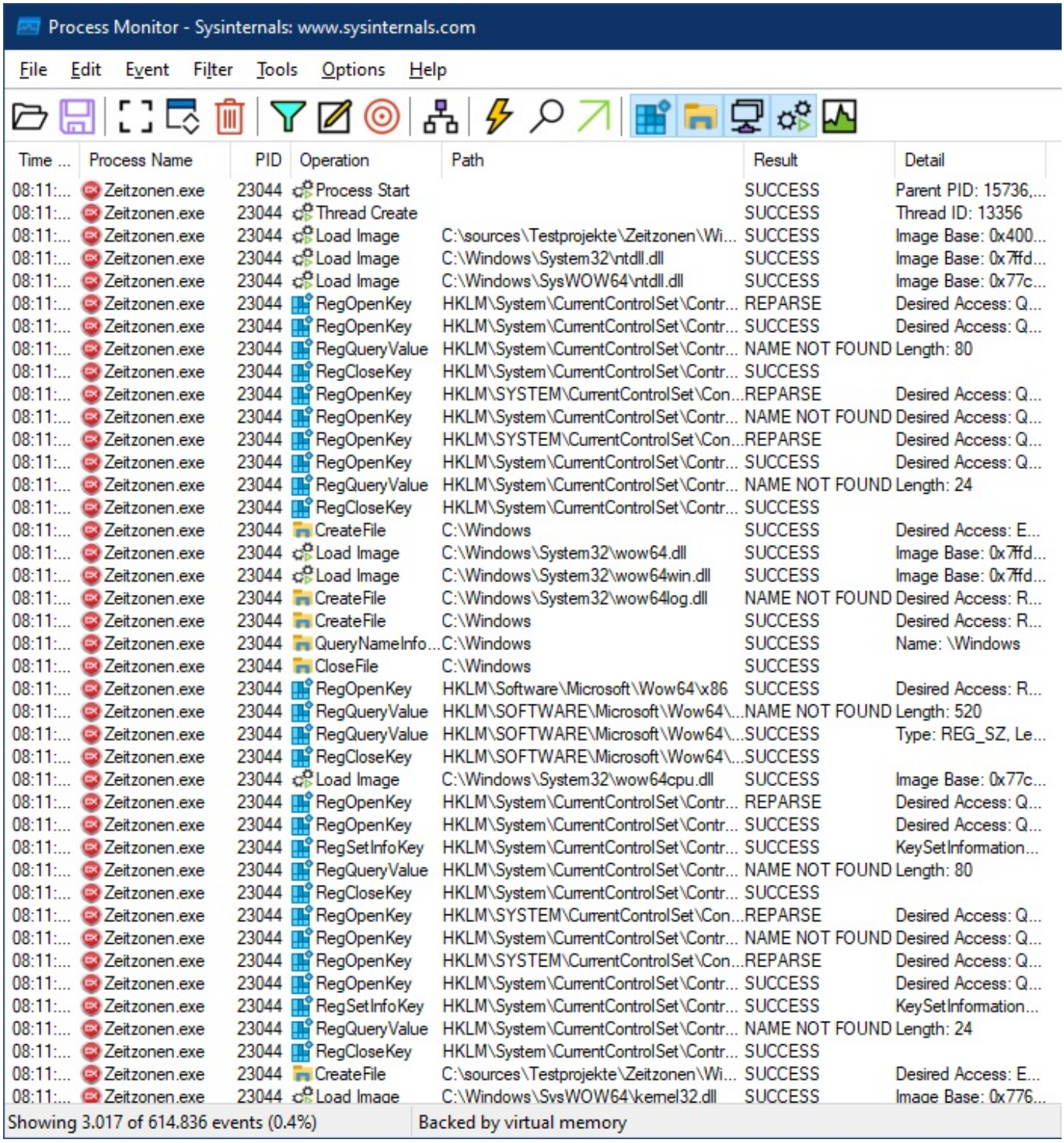
- Nun können Sie alle bislang aufgezeichneten **Einträge** über einen Klick auf das Clear-Icon oder die Tasten-Kombination Strg + X leeren.

- Nehmen wir an, wir möchten den Prozess bzw. das **Programm** Zeitzonen.exe überwachen.
- Damit nur die Aufzeichnungen zu diesem Prozess angezeigt werden, legen wir über einen Klick auf das Filter-Icon oder die Tastenkombination Strg + L einen **Filter** dafür an (es öffnet sich das Fenster Process Monitor Filter).

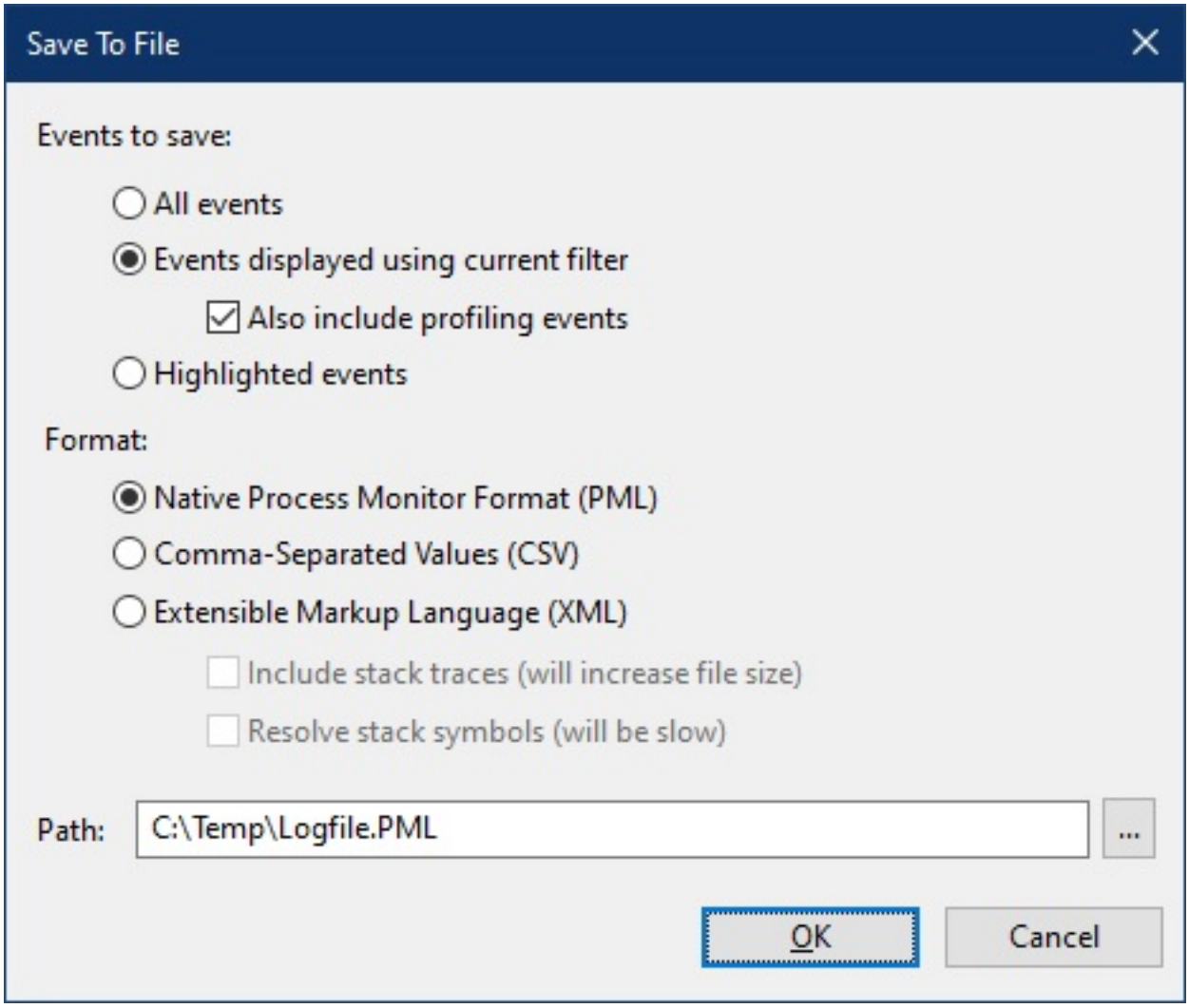
- Hier legen wir einen neuen Filter an, der sich auf den Prozess-Namen Zeitzonen.exe bezieht, und fügen diesen über **Add** hinzu (bitte beachten, dass das Häkchen gesetzt ist, so dass der Filter auch aktiv ist).



- Wichtig: Die übrigen **Exclude**-Bedingungen in diesem Fenster sorgen dafür, dass das Programm **Process Monitor** sich nicht selbst überwacht und sollten daher alle aktiv bleiben (Häkchen sind weiterhin gesetzt).
- Nun starten wir die **Aufzeichnung** über einen Klick auf das Capture-Icon oder über die Tastenkombination Strg + E.
- Anschließend **starten** wir unser Programm Zeitzonen.exe, damit die Aufzeichnung über diesen Prozess beginnen kann.
- Nun führen wir in unserm Programm Zeitzonen.exe alle Aktionen aus, die wir überprüfen möchten (z.B. diejenigen, die sehr langsam sind, und die wir daher überwachen möchten, oder diejenigen, die **Probleme** verursachen).
- Abschließend schließen wir das Programm und beenden die **Aufzeichnung** über einen Klick auf das Capture-Icon oder über die Tastenkombination Strg + E.
- **Process Monitor** gibt uns nun ausführliche **Informationen** darüber, wann z.B. Dateien erstellt wurden, Bilder geladen wurden, Registry-Zugriffe erfolgt sind etc.



- Über einen Klick auf das Save-Icon (Diskette) oder die Tastenkombination Strg + C können wir die Ergebnisse der Aufzeichnung zur genaueren Auswertung als **Datei** speichern (es öffnet sich das Fenster Save To File).



- Dies ist nur ein kleiner Auszug der Möglichkeiten, die Ihnen mit **Process Monitor** zur Verfügung stehen, für genauere bzw. detailliertere Informationen sehen Sie sich die **Hilfe** bzw. die **Dokumentation** an.

Eindeutige ID: #2619
Verfasser:
Letzte Änderung: 2022-09-05 12:56