DIETMAR **W**ALKER - **P**C-**B**LITZHELFER-**N**OTDIENST
Nationalgasse 14 • **7**2124 **P**liezhausen • ∅ **T**el. 07127 / 890 729 - **F**ax 89118
Internet: http://www.pc-blitzhelfer.de – **M**obil 0172-882 79 55

Anleitung Process Monitor- Anleitung und Tutorial zum Profi-Analysewerkzeug

Der Process Monitor loggt vermutlich sämtliche Dateisystem- und Registry-Zugriffe, sowohl lesende als auch schreibende. Wir liefern Grundlagentipps für versierte Einsteiger.
Mitunter lesen Sie in einem Artikel davon, ein Programm sei ein "Profi-Tool". Vielfach ist das zu hoch gegriffen. Auf den **Process Monitor** aber trifft diese Beschreibung voll und ganz zu: Er stammt von einem Profi – Mark Russinovich, der mittlerweile für Microsoft arbeitet – und richtet sich an Profis. Vor diesem Hintergrund eine Warnung zu dem portablen System-Tool: Haben Sie keine hohe Frustrationstoleranz und nicht allzu viel Zeit, ist das Monitoring-Programm nichts für Sie. Denn man benutzt es nicht einfach so, vielmehr sollten Sie ein konkretes Anliegen haben, wobei Ihnen der Process Monitor dann mit ergiebigen Datensätzen zur Seite steht. Das Programm erfasst wohl alle schreibenden und lesenden Dateisystem- und Registry-Zugriffe und stellt sie in einem stetig anwachsenden Protokoll bereit. So blicken Sie (auf Wunsch in Echtzeit) in das durchaus komplexe Windows-Fundament. Neben Einblicken in die Arbeitsweise Ihres Betriebssystems kommen Sie so Problemen auf die Spur.
Process Monitor herunterladen
Download

Voraussetzungen zur sinnvollen Nutzung

PC-Anfänger sollten Process Monitor nicht laden, sie können mit dessen angezeigten Daten (nahezu) nichts anfangen. Versierte und interessierte Anwender wiederum profitieren von dem Tool. Einige Skills und etwas Background zu Windows eignen Sie sich mithilfe des Artikels "Windows-Begriffe von A bis Z: Der ultimative Einblick ins Betriebssystem" an. Auch ein Blick in unsere Ratgeber zu Dateisystemen, Registry und Batch-Programmierung schadet nicht.
Mit dem Process Monitor blicken Sie tief in Windows hinein: Das Programm zeichnet wohl alles auf, was sich im Hintergrund abspielt. Das Utility macht unsichtbare Vorkommnisse sichtbar: Beinahe jeder Ihrer Mausklicks löst (mindestens) eine (oft kleinteilige) Aktion aus. Davon bemerken Sie im Windows-Betrieb nichts – das ist fein, denn so ist eine gute Bedienbarkeit gewährleistet.
Schon ein einfacher Dateiaufruf tritt viele Aktionen los, die sich in einer Vielzahl an Einträgen im Process Monitor manifestieren. Noch mehr spielt sich hinter den Kulissen (die der Process Monitor Ihnen offenbart) ab, wenn Sie Programme starten: Die bestehen nämlich in der Regel aus gleich mehreren Dateien; sie alle gelangen bei Softwarestarts von der Festplatte beziehungsweise SSD ins RAM. Programme rufen ihre Einstellungen außerdem meist aus der Registry ab (portable Applikationen beziehen sie hingegen etwa aus INI-Dateien) und schreiben teils in die Datenbank, zum Beispiel geänderte Einstellungen. Die vielen Zugriffe betreffen ebenso Windows selbst: Auch das Betriebssystem ist ein Programm; wenn Sie beispielsweise per Klick in den Windows-Ordneroptionen (control folders) eine Einstellung ändern, speichert das System sie in der Sammelstelle für Konfigurationswerte – in der Registry. Faktisch löst also ein Klick in den Ordneroptionen auf die Schaltfläche "Übernehmen" oder "OK" einen schreibenden Registry-Zugriff aus. Der Process Monitor weist das nach. Wie Sie hier eigene Experimente wagen, erläutert dieser Artikel.

Process Monitor vs. Process Explorer

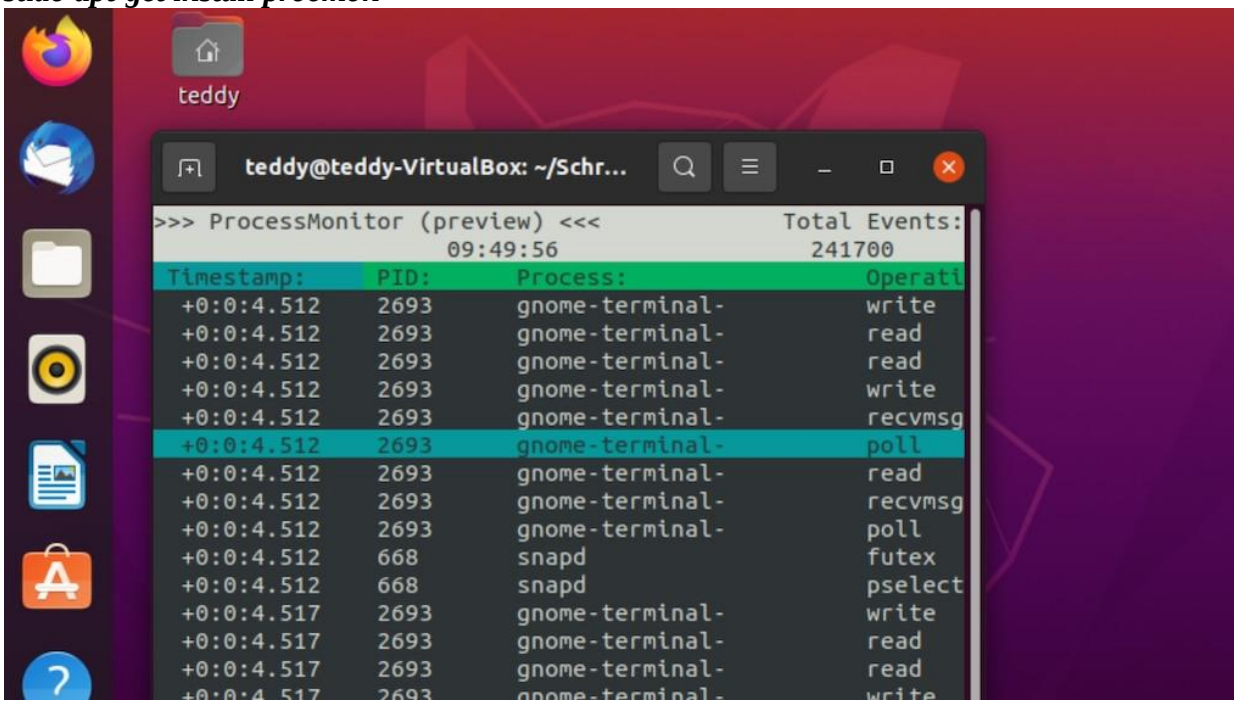
Wollen Sie sich auf die Suche nach Leistungsräubern im Arbeitsspeicher begeben, decken Sie entsprechende Programmprozesse mit dem Process Explorer (Procexp) noch besser auf. Das Programm ist eine Alternative zum Task-Manager. Der Process Explorer ist eher ein Tuning-

Tool als der Process Monitor. Letzterer geht allenfalls leicht in diese Richtung und siedelt sich thematisch beim Task-Manager an – in seiner Paradedisziplin ist der Process Monitor ein Prozesse-Logger und mehr Zusatz zum Task-Manager als Ersatz.

Recht neu: Process Monitor für Linux

Ein Tipp für Linux-Anwender: Auf Microsofts zugekaufter Entwicklerplattform GitHub gibt es Procmon auch für Ubuntu, Details und Installationsanweisungen finden Sie auf der zugehörigen Projektseite. Die Procmon-Installation ist von Microsoft für Ubuntu 18.04 LTS und Ubuntu 20.04 LTS vorgesehen. In unserem Test mit der neueren langzeitunterstützten Ubuntu-LTS-Variante 20.04 funktionierte die Einrichtung problemlos; bei Ubuntu 21.04 scheiterte sie. Tipps zur Windows-Alternative Ubuntu finden Sie im Artikel "Linux Ubuntu: Anfänger-Tutorial mit 31 Einstiegstipps, auch zur Installation". Die Kurzform der Procmon-Installation unter Ubuntu: Klicken Sie mit der rechten Maustaste auf eine freie Schreibtisch-Fläche (Schreibtisch heißt im Ubuntu-Jargon der Desktop) und wählen Sie "Im Terminal öffnen" im Kontextmenü. Es folgt die Eingabe von vier Befehlen, die Microsoft auf der oben verlinkten GitHub-Projektseite nennt:

wget -q https://packages.microsoft.com/config/ubuntu/$(lsb_release -rs)/packages-microsoft-prod.deb -O packages-microsoft-prod.deb
sudo dpkg -i packages-microsoft-prod.deb
sudo apt-get update
sudo apt-get install procmon

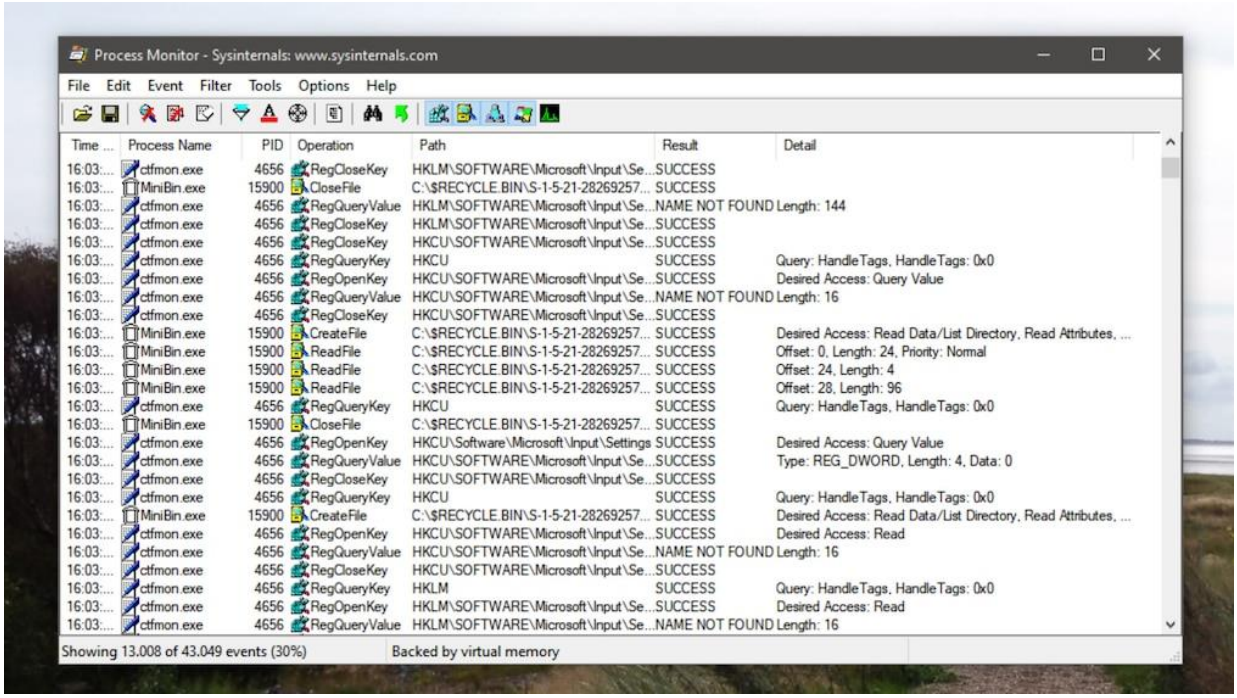


Der Process Monitor kommt unter Windows sicherlich häufiger als unter Ubuntu zum Einsatz. Dennoch beeindruckt es, wie sich Microsoft dem quelloffenen Linux immer mehr öffnet.
Nun lässt sich der Process Monitor per Terminal als Konsolen-Anwendung starten, also ohne GUI (**G**raphical **U**ser **I**nterface, grafische Benutzeroberfläche). Dem dient der Befehl ***sudo procmon***. Das sudo verschafft der Anwendung dabei, wie bei Linux Ubuntu üblich, erhöhte Rechte, vergleichbar mit denen von Administrator-Benutzerkonten unter Windows. Da Windows die weitaus verbreitetere Plattform ist, geben wir nachfolgend Tipps zum Einsatz des Process Monitors unter diesem Betriebssystem.

DIETMAR **W**ALKER - **P**C-**B**LITZHELFER-**N**OTDIENST
Nationalgasse 14 • **7**2124 **P**liezhausen • ∅ **T**el. 07127 / 890 729 - **F**ax 89118
Internet: http://www.pc-blitzhelfer.de – **M**obil 0172-882 79 55

Windows: Process Monitor downloaden

Den Process Monitor laden Sie für Windows sowohl stand-alone (alleinstehend) als auch als Teil der Sysinternals Suite herunter. Letztere bündelt in einem ZIP-Archiv rund 70 zu entpackende systemnahe Hilfstools; mit dabei sind Process Monitor und Process Explorer. In unserem Stand-alone-ZIP-Download finden Sie drei ausführbare Dateien: Procmon.exe als 32-Bit-Version (läuft auch unter Windows 64 Bit), Procmon64.exe als 64-Bit-Version und Procmon64a für ARM-CPU-PCs. Die letztere Fassung ignorieren Sie, diese startet auf Ihrem Computer vermutlich nicht. Im Gepäck hat das ZIP-Paket ferner eine Eula.txt-Datei und eine procmon.chm-Hilfedatei. Beim Aufruf einer der EXE-Files erscheint eine Warnmeldung der Benutzerkonten-Steuerung, bestätigen Sie sie mit einem Klick auf "Ja". Sodann poppt ein EULA-Fenster von Process Explorer auf. Darin stimmen Sie den Nutzungsbedingungen per Klick auf "Agree" zu. Das ist nur einmal nötig, danach nicht mehr; denn Process Monitor vermerkt in der Registry im neu angelegten Schlüssel HKEY_CURRENT_USER, SOFTWARE, Sysinternals und dort im Unterschlüssel "Process Monitor" per DWORD-Eintragswert EulaAccepted via Wert 1, dass Sie zugestimmt haben.
Möchten Sie den Process Monitor über die Sysinternals Suite beziehen, laden Sie diese zunächst herunter. Alternativ zu einem normalen Download hängen Sie die Suite als FAT-formatiertes Netzlaufwerk in Windows ein: Starten Sie eine Kommandozeile ohne (!) Administrator-Rechte, indem Sie Win-R drücken und *cmd* eingeben. Lassen Sie das Kommando folgen:
net use X: http://live.sysinternals.com/tools
Nun steht im Explorer unter dem Laufwerksbuchstaben X ein neuer Speicherbereich bereit, aus dem Sie per Doppelklick Tools wie den Process Monitor aufrufen. Auch das Kopieren dortiger (EXE-)Dateien zum Beispiel auf den Desktop ist möglich. Möchten Sie das von Hand abwickeln, wenden Sie Drag & Drop an. Puristen kopieren das File per Kommandozeile:
copy X:\Procmon64.exe %userprofile%\Desktop
Am Ende hängen Sie das Netzlaufwerk wieder aus. Um es zu trennen, verfrachten Sie in die CMD den folgenden Befehl:
net use X: /delete



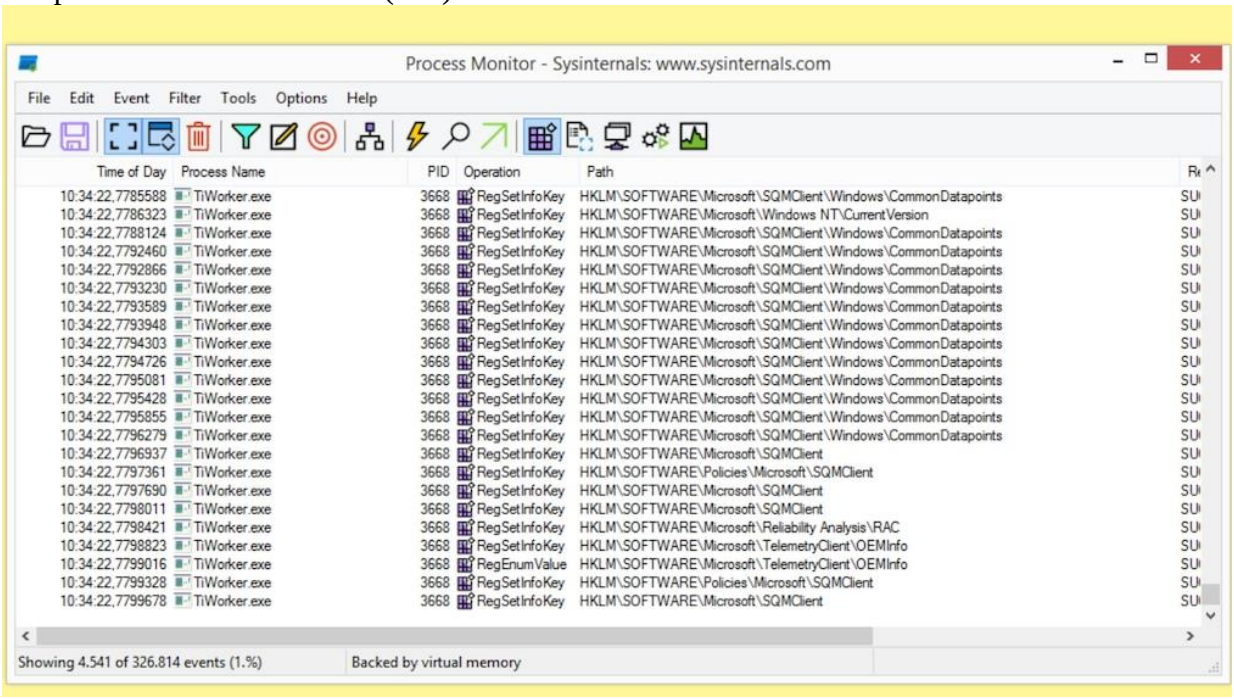
Der Tiefgang beim Process Monitor ist erquickend. Zugleich stellt er aber die größte Schwäche der Anwendung dar – in ihrem Informationswust durchzusteigen, will gelernt sein.

Erste Schritte mit dem Process Monitor

Gleich nach dem Start trägt der Process Monitor zahlreiche Einträge zusammen – und es werden von Sekunde zu Sekunde mehr. Bei diesen großen Datenmengen bei PC-Problemen oder zum Erforschen von OS-Verhaltensweisen das Gewünschte zu finden, gleicht der berühmt-berüchtigten Nadel-Suche im Heuhaufen. Daher gibt es Filterfunktionen. Diese und die zahlreichen Daten in Gänze zu verstehen, erfordert ein eingehendes Studium der Anwendung. Da kaum jemand diesen Aufwand betreiben will, kommen Sie durch Ausprobieren und Fehlschläge (Trial and Error) irgendwann ans Ziel – oder auch nicht, was manchmal geschieht. Mitunter hilft Ihnen eine Suche im Internet, die richtigen Infos aufzustöbern und gefundene korrekt zu interpretieren. Im Übrigen wirkt der Process Monitor nicht zerstörerisch, denn er analysiert zwar umfassend quasi alles, greift darüber hinaus aber nicht näher ins Betriebssystem ein.

1. Starten Sie den Process Monitor (Pocmon) per Doppelklick auf Procmon(64).exe. Bestätigen Sie gegebenenfalls (einmalig nötig) per Klick auf "Agree". Die Benutzerkonten-Steuerung nicken Sie mit "Ja" ab.
2. Das Programm loggt zahlreiche Ereignisse, deren Gesamtzahl lesen Sie im unteren Fensterbereich ab. Zugleich steigt der RAM-Verbrauch von Procmon, was ein Blick in den Windows-Task-Manager offenbart.
3. Möchten Sie dem Arbeitsspeicher-Verbrauch Einhalt gebieten und das Loggen weiterer Vorkommnisse stoppen, klicken Sie in der Symbolleiste oben auf das Capture-Symbol (das dritte von links). Die Anzahl protokollierter Vorkommnisse erhöht sich nun nicht mehr (siehe den unteren Fensterbereich). Möchten Sie das Zusammentragen von Protokolleinträgen fortsetzen, gelingt Ihnen das durch erneutes Anklicken des Capturing-Icons.
4. Die Symbole in der Icon-Leiste oben im Process Monitor sind nicht selbsterklärend. Der Kritikpunkt, dass sie optisch angestaubt sind, gilt aber nicht mehr, denn Microsoft hat dem Tool im Jahr 2021 ein Update verpasst. Führen Sie sich die Funktionen der Symbol-Palette zu Gemüte, indem Sie den Mauszeiger auf die Icons bewegen. Jeweils poppt eine Quickinfo auf, die Ihnen englischsprachig den Namen der Funktion und dahinter in Klammern die zugehörige Tastenkombination anzeigt.
Die Hotkeys sind bei der Arbeit mit dem Programm wichtig: Mitunter ist es nämlich nötig, eine Funktion schnell anzuwenden. Um beispielsweise rasch das Loggen zu starten und wieder zu pausieren, sind Mausklicks nicht maximal effizient. Flotter sind Sie hier mit Strg-E unterwegs. Zum Löschen aller Einträge klicken Sie auf das fünfte Symbol von links (den Papierkorb) oder Sie drücken Strg-X. Der Process Monitor legt jetzt gleich wieder Einträge an, wenn er noch im Protokoll-Modus ist oder wenn Sie ihn wieder aktivieren.
5. Oben rechts finden sich fünf Symbole: Die gehören zu den Filterfunktionen. Per Klick auf die Icons bewirken Sie, dass der Process Monitor die zugehörigen Informationen nicht mehr anzeigt. Die Quick-Info-Erklärungen bei Mouse-overn lauten (von links nach rechts) "Show Registry Activity", "Show File System Activity", "Show Network Activity", "Show Process and Thread Activity" und "Show Profiling Events". Wenn die Icons farbig unterlegt sind, sehen Sie die zugehörigen Infos im Process Monitor; nach dem Anklicken sind die Symbole nicht mehr visuell hervorgehoben und so fallen ihre Daten aus der langen Tabelle heraus. Dies ist ein guter Weg, um die Eintragsliste zu entschlacken. Wobei der Process Monitor von dem Angezeigten Ausgeklammertes weiterhin protokolliert: Es ist nur nicht in Ihrem Sichtfeld.
Je nachdem, welche Bereiche Sie sich anzeigen lassen, variiert im unteren Bereich die "Showing X of Y events"-Angabe. Dabei ist X so hoch, wie die Anzahl der Einträge innerhalb

der oben aktivierten Rubriken; wohingegen Y der Gesamtzahl aller geloggten Vorkommnisse entspricht und sich durch das (De-)Aktivieren der Filter-Icons nicht verändert.



Die Einträge oben rechts sind nicht sämtliche, aber doch wichtige Filter im Process Monitor. Mit ihnen machen Sie sich das Leben durch eine Reduktion der Einträge leichter.

Process Monitor: Einfache Beispiele

Um die Funktionsweise von Process Monitor zu verstehen, eignen sich die folgenden Beispiele. Mit denen schöpfen Sie die Möglichkeiten beileibe nicht aus, erhalten aber ein besseres Verständnis:

1. Stellen Sie sicher, dass der Process Monitor protokolliert. Öffnen Sie den Windows-Editor mit Win-R und *notepad* und erzeugen Sie mit ihm eine TXT-Datei. Speichern Sie sie beispielsweise unter dem Namen diesdasananas.txt im Dokumente-Ordner. Tipps zu Notepad finden Sie übrigens hier.
2. Drücken Sie im Process Monitor Strg-E, um das Logging zu unterbrechen.
3. Drücken Sie im Programm Strg-F, um die Suchfunktion aufzurufen.
4. Geben Sie "diesdas" ein und bestätigen Sie mit der Eingabetaste.
5. Sie sollten auf mehrere Funde stoßen, die der Dateierstellung zugehörig sind. Mit dabei ist unter anderem ein "CreateFile"-Eintrag, bei dem in der "Path"-Spalte beim Windows-Benutzernamen teddy beispielsweise Folgendes steht: "C:\users\teddy\Documents".
6. Auch wenn Sie die Dateierzeugung per Kommandozeile vornehmen, gelangen Sie an entsprechende Infos. Zum Erstellen eines TXT-Dokuments via cmd.exe geben Sie in die Konsole zum Beispiel das Folgende ein: *echo BeliebigerInhalt > %userprofile%\Documents\diesdasananas12345.txt*
7. Es bietet sich an, testweise mit Editor (notepad.exe), Paint (mspaint.exe) und Kommandozeile (cmd.exe) Dateien zu speichern. Suchen Sie im Process Monitor jeweils mit Strg-F nach dem Dateinamen, stoßen Sie auf zugehörige Einträge. In der Spalte "Process Name" sehen Sie dabei jeweils die Anwendung, die den Dateisystem-Zugriff getätigt hat: Bei mspaint.exe etwa findet sich links neben dem Programmnamen das zugehörige Anwendungs-Icon.

8. Auch Programmstart-Zeitpunkte lassen sich nachvollziehen: Fahnden Sie via Strg-F nach einem Prozess wie firefox.exe oder opera.exe, sehen Sie mehrere Einträge. Bei den Suchfunden erkennen Sie anhand eines Datum-Zeitstempels bei "Time of Day", um wie viel Uhr der Prozess ins RAM gelangte. Bei der Sekundenangabe gibt es mehrere Nachkommastellen. Was unsinnig wirkt, ist für Profis sinnvoll: Ein Mausklick, der beispielsweise eine Registry-Änderung lostritt, bewirkt verschiedene Aktionen. Sie alle gelangen ins Protokoll. In welcher Reihenfolge sich was abgespielt hat, erschließt sich anhand der Millisekunden. Per Doppelklick auf einen der Einträge öffnen Sie seine Eigenschaften: Im Beispiel von Firefox lesen Sie auf der Registerkarte "Process" unter anderem die PID (Process-ID-Nummer) und den EXE-Pfad ab.
9. Ganz allgemein sehen Sie, wenn Sie den EXE-Programmnamen eines Programms eingeben, die ihm zugehörigen Einträge. Der Process Manager teilt Ihnen dann reichlich technisch mit, was die Anwendung alles getan hat. Wohlgemerkt: innerhalb der Zeit, in der die Aufzeichnung von Process Monitor aktiv war. Effektiver ist es häufig, die Einträge auf eine bestimmte Anwendung zu beschränken: Oben finden Sie ein rotes Jagd-Symbol. Das klicken Sie an und Sie bewegen den Mauszeiger bei gedrückter Maustaste auf das Programmfenster, dessen Prozess zu analysieren ist. Wichtig ist, dass ein schwarzer Kasten zu sehen ist, egal wo. Dann lassen Sie die Cursor-Taste los und es geht in Procmon erheblich übersichtlicher zu; für ergiebige Infos schalten Sie oben rechts keine Filter aktiv, es sei denn, Sie suchen nach etwas Bestimmtem. Beachten Sie, dass der Process Monitor nun nichts anderes mehr anzeigt; die Filterung heben Sie per Neustart von Procmon und Klicks im Start-Pop-up auf "Reset > OK" (nicht bloß auf "OK") auf. Möchten Sie auf den Procmon-Neustart verzichten, erreichen Sie alternativ mit Strg-R das Entfernen aller Ihrer Filter.

Process Monitor: Ein Registry-Detektiv-Spiel

Wenn Sie in Windows per Klick eine Einstellung ändern, modifiziert das Betriebssystem in der Regel im Hintergrund der Registry. Dabei ändert es etwa den Wert eines DWORD-Wert-Eintrags. Möchten Sie herausfinden, welcher interne Eingriff genau mit einem Mausklick korrespondiert, ist Ihnen das Internet behilflich. Es genügt, einen Einstellungsnamen zusammen mit dem Begriff "regedit" zu googeln. Doch stimmen die Infos im Web tatsächlich? Das finden Sie durch einen Blick in den Registry-Editor heraus: Sie starten dieses Bordmittel regedit.exe, navigieren dort zur vermeintlich zugehörigen Stelle, ändern in Windows per GUI/Klick die gewünschte Einstellung und aktualisieren in regedit mit der F5-Taste die Ansicht. Der Registry-Wert sollte sich geändert haben. Auch der Process Monitor ist Ihnen bei der Recherche behilflich: Mit ihm decken Sie mit einigem Spürsinn Registry-Modifikationen auf. Eine Internet-Anleitung brauchen Sie dann nicht erst mit Google, Bing & Co. aufzustöbern. Klappt alles, nutzen Sie die gewonnene Erkenntnis zu einem geänderten Registry-Eintrag, um den Inhalt in einer REG- oder Batch-Datei unterzubringen. So wenden Sie die Modifikation später (auf Ihrem PC nach einer Windows-Neuinstallation oder an einem fremden Gerät) blitzschnell an.
1. Dieses Beispiel behandelt eine Änderung der Windows-Ordneroptionen. Diese rufen Sie mit Win-R und *control folders* auf. Das Folgende haben wir, ebenso wie den Rest des Artikels, unter Windows 8.1 und Windows 10 21H1 recherchiert. Wechseln Sie auf die Registerkarte "Ansicht". Dort finden Sie recht weit unten die Option "Ausgeblendete Dateien, Ordner und Laufwerke anzeigen". Genau die Änderung, die sich an der Windows-Registry durch das Setzen eines Radiobutton-Punkts vor der Option (samt Bestätigung per "Übernehmen"- oder "OK"-Button) ergibt, wollen wir im Beispiel in eine Batch-Datei gießen.
2. Setzen Sie einen Punkt vor "Ausgeblendete Dateien, Ordner und Laufwerke anzeigen". Aber: Setzen Sie die Einstellungsänderung noch nicht mit "Übernehmen" oder "OK" in die Tat um.

Holen Sie zuvor den Process Monitor nach vorn. Gleich klicken Sie auf die "Übernehmen"-Schaltfläche (Vorteil im Vergleich zum OK-Button: Die Ordneroptionen schließen sich nicht); darauf bereiten Sie sich erst noch vor. Da beim Anklicken zahlreiche neue Einträge (auch viele irrelevante, die aufgrund anderer PC-Ereignisse entstehen) Einzug in den Process Monitor halten, löschen Sie vorbereitend das bislang im Tool angesammelten Log: Pausieren Sie das Datensammeln für einen ruhigen Blick (Strg-E) und drücken Sie Strg-X zum Entfernen des Datensatzes.

3. Spielen Sie die folgenden Aktionen eventuell ein paar Mal durch, um sie schnell anzuwenden: Mit einem Klick auf das Capture-Symbol (das dritte von links) aktivieren Sie, dass der Process Monitor jedwede PC-Aktivitäten aufzeichnet. Schneller ist es, Strg-E zu drücken. Ohne Umschweife klicken Sie im Ordneroptionen-Fenster danach auf "Übernehmen". Möglichst wieder ohne zeitlichen Verzug beenden Sie das Loggen, indem Sie ins Procmon-Fenster klicken und Strg-E drücken. Je weniger Zeit das alles in Anspruch nimmt, desto besser: Denn die an Windows vorgenommene Registry-Änderung gelangt, während Sie bei aktiviertem Logging in control folders klicken, ins Procmon-Protokoll; darüber hinaus kommen hunderte Aktivitäten mehr hinzu. Die interessieren hier nicht. Würden Sie mehr Zeit als nötig aufwenden, fällt das Durchsuchen des Datensatzes schwerer; die Nadel im Heuhaufen wäre noch zeitaufwendiger aufzustöbern als ohnehin schon.
Ein Vorschlag für das fixe Bedienen: Platzieren Sie die Ordneroptionen und den Process Monitor nebeneinander. Setzen Sie das Procmon-Fenster per Klick in den Fokus und bewegen Sie den Mauszeiger auf die Ordneroptionen-"Übernehmen"-Schaltfläche. Drücken Sie Strg-E, was sich auf Procmon auswirkt. Danach klicken Sie per linker Maustaste, womit Sie den Button "Übernehmen" (innerhalb der Ordneroptionen) erwischen. Klicken Sie nun schnell ins Procmon-Fenster, um die Aufzeichnung mit Strg-E gleich wieder zu beenden. Mit flinken Fingern dauert das alles nur circa eine Sekunde.

4. Der Process Monitor hat ein paar Tausend Einträge aufgezeichnet. Händisch lassen sich diese nicht sinnvoll durchstöbern, schließlich wollen Sie nicht die ganze Nacht damit verbringen. Daher reduzieren Sie die Einträge mithilfe der Filter-Icons oben rechts: Da Sie einen Registry-Hack recherchieren wollen, klammern Sie die Ereignis-Kategorien, die nichts damit zu tun haben, aus: Klicken Sie alle Rubriken-Icons bis auf das ganz links an. Die Anzahl der Einträge schrumpft so (je nach System) um mehrere Hundert bis Tausend.

5. Anhand des Zeitstempels in der Spalte links kommen Sie dem Registry-Schlüssel, in dem sich die Registry-Modifikation abspielt, theoretisch auf die Spur. Praktisch funktioniert das mit vertretbarem Zeitaufwand aber nicht: Denn schon binnen einer Sekunde kommen Tausende Einträge zusammen. Es sind noch immer zu viele Einträge. Also müssen Sie sie weiter reduzieren.

6. Eine Suche im Internet wollten wir eigentlich nicht durchführen, wir schummeln nun aber doch: Eine Bing-Suche ergab, dass die Ordneroptionen-Option "Ausgeblendete Dateien, Ordner und Laufwerke anzeigen" eine Registry-Modifikation im folgenden Schlüsselpfad bewirkt:
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced
Dort gibt es einen Registry-Eintrag "Hidden", der beim Ausblenden versteckter Dateien den Wert 2 hat – und beim Einblenden der Files (also beim Anwenden des Ordneroptionen-Tweaks) den Wert 1. Das ist also der Registry-Inhalt, den wir am Ende idealerweise herausfischen.

7. Die per Internet-Recherche ermogelte Erkenntnis bringt uns beim Filtern mit dem Process Monitor voran: Da sich der Tweak in HKEY_CURRENT_USER (HKCU) abspielt, für dessen Bearbeitung per Batch es übrigens keine Administrator-Rechte braucht, sind etwa HKLM-Registry-Abschitte (HKEY_LOCAL_MACHINE) irrelevant. Blenden wir die aus, reduziert sich die Anzahl der Einträge ein gutes Stück: Klicken Sie einen der Einträge in der Spalte

"Path" mit der rechten Maustaste an, erscheint ein Kontextmenüeintrag mit "Exclude" im Namen. Das, was hinter dem "Exclude" steht, schließen Sie durch das Setzen eines Filters aus. Je nachdem, ob Sie einen Eintrag unerwünschten Typs in der "Path"- oder "Operation"-Spalte rechtsklicken, differiert das genau angebotene Exclude-Angebot. Um zum Beispiel sämtliche HKLM-Einträge zum Verschwinden zu bringen, klicken Sie einen beliebigen HKLM beinhaltenden Eintrag in der "Path"-Spalte mit der rechten Maustaste an und wählen "Edit Filter (...)". Im sich öffnenden Fenster definieren Sie die "conditions", also die Bedingungen zum Ausblenden. Lassen Sie "Path" unverändert, rechts davon wählen Sie per Drop-down-Menü (statt "is") "contains". Ins Eingabefeld rechts daneben tippen Sie "HKLM". Im Drop-down-Menü ganz rechts stellen Sie sicher, dass "Exclude" gewählt ist. Bestätigen Sie mit "Add > OK".

8. Das Ausblenden von Registry-Protokoll-Einträgen treiben Sie noch ein gutes Stück weiter – mit entsprechendem Vorwissen: Registry-Wert-Änderungen triggern im Process Monitor das Anlegen eines Eintrags vom Typ "RegSetValue". Genau so einen Eintrag wollen Sie finden und Sie dürfen den Typus nicht ausklammern. Doch Einträge, die mit dem Ordneroptionen-Hack in Verbindung stehen, aber nicht der exakt gesuchte sind, brauchen Sie nicht. Auch sind die vielen Einträge jenseits des Windows-Hacks entbehrlich.

Daher machen Sie kurzen Prozess mit Nicht-RegSetValue-Einträgen: Rechtsklicken Sie etwa einen "RegCloseKey"-Eintrag in der "Operation"-Spalte und schließen Sie ihn samt weiterer Einträge dieses Typs per "Excluce RegCloseKey"-Kontextoption aus. Wiederholen Sie das Ausmisten mit hier weiteren unnützen Inhalten etwa der "RegEnumKey"-, "RegOpenKey"-, "RegQueryValue" oder "RegQueryKey"-Klassifizierung.

9. Am Ende ist der Einträge-Bestand kräftig ausgedünnt: Ehemals mehrere Tausend Vorkommnisse sind auf weniger als 100 zusammengeschrumpft. Je nach PC und der Anzahl Ihrer Filterungen sind es womöglich mehr Einträge. In jedem Fall sollte es leichter fallen, den Datenbestand manuell zu sichten. Auf Wunsch ist Ihnen die Suchfunktion mit Strg-F behilflich. Der gefundene Eintrag im Beispiel lautet wie folgt:

RegSetValue
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Hidden

Als Result ist "SUCCESS" angegeben, der Process Monitor verrät in der "Detail"-Spalte: "Type: REG_DWORD, Length: 4, Data: 1"

Der Teil "Data: 1" meint dabei, dass der Registry-Wert auf 1 geändert wurde. Eine weitere Spielwiese für Procmon-Experimente mit geänderten Registry-Einstellungen bieten die Windows-Leistungsoptionen: Dort aktivieren Sie auf dem Tab "Visuelle Effekte" etwa "Benutzerdefiniert", in der Folge trägt Windows in einem Registry-Eintrag VisualFXSetting den Wert 3 ein (was Procmon mit "Length: 4, Data: 3" attestiert). Das Geniale: Haben Sie die Filter wie oben beschrieben erst einmal gesetzt, brauchen Sie das nicht zu wiederholen und weitere Registry-Recherchen gestalten sich recht kurzweilig. Englisch sollten Sie rudimentär beherrschen, sonst müssen Sie bei den verbliebenen paar Dutzend englischsprachigen Protokolleinträgen raten, welche Phase zu genau Ihrem Tweak gehört. Die nötigen Kenntnisse vorausgesetzt, münzen Sie solche Eintragswert-Änderungen in eine Batch-Datei um. Oder Sie erstellen im Windows-Registry-Editor ein REG-Skript – das leistet Ähnliches wie eine Batch-Datei und die Erstellung bei REG geht einfacher (wenige Klicks nötig).

PS: Die oben beschriebene Recherche erleichtern Sie sich, wenn Sie einen zweiten PC besitzen. Auf dem sollte möglichst ein frisches Windows installiert sein. Jede installierte und im Hintergrund aktive Software bläht die Procmon-Protokolle weiter auf, was Ihnen die Arbeit erschwert. Das bedeutet aber nicht, dass Procmon auf PCs mit schon vorhandenem Softwarebestand unnötig wäre: Das Gegenteil ist der Fall – zur Höchstform läuft die Applikation auf, wenn Sie Probleme haben und denen auf den Grund gehen wollen. Solide

Windows-Kenntnisse sind aber die Voraussetzung, womöglich ist aber eine Windows-Neuinstallation fürs Troubleshooting schneller vollzogen.

Weitere Process-Manager-Tipps

Der Process Monitor zeigt auch Programme an, die mit UDP-Verbindungen online gehen: Beschränken Sie mit den Filter-Icons oben rechts die Anzeige auf "Network Activity", sehen Sie etwa, dass sich Google Chrome mit dem Internet verbindet. Procmon beherrscht sogar das Aufzeichnen von Windows-Interna beim Bootvorgang; so weisen Sie nach, dass das Betriebssystem verwaiste Registry-Einträge zu laden vermag. Details finden Sie im Artikel "Windows: Registry aufräumen, sichern, einstellen".
Ein Tipp zum Schluss: Womöglich waren Sie beim Setzen der Procmon-Filter übereifrig, dann sehen Sie bestimmte wichtige Einträge nicht mehr. Das macht nichts: Starten Sie den Process Montor einmal neu, öffnet sich ein Fenster zur Filter-Konfiguration. Dort klicken Sie auf die Schaltfläche "Reset" und bekommen daraufhin wieder vollumfänglich die geloggten Datenschätze zu Gesicht.

Quelle: https://www.computerbild.de/artikel/cb-Tipps-Software-Process-Monitor-Anleitung-und-Tutorial-zum-Profi-Tool-29726769.html